现代数学基础丛书　103

椭圆曲线公钥密码导引

祝跃飞　张亚娟　著

科 学 出 版 社

北 京

内 容 简 介

椭圆曲线是一门古老而内容丰富的数学分支，ECC 理论涉及了许多深奥的椭圆曲线算数理论，要系统详细地讲授 ECC 理论需要较深的数学基础. 本书的目的是在交换代数的基础上系统阐述 ECC 理论，为有志于从事该方向研究的人员提供一本系统全面的基础性教材. 本书围绕 ECC 的理论和实践分三部分：第一部分介绍椭圆曲线的算术理论，主要是有限域上椭圆曲线的相关理论；第二部分为 ECC 的密码理论，重点论述了有限域上椭圆曲线的求阶算法，椭圆曲线上的离散对数求解算法和椭圆曲线公钥密码体制，椭圆曲线的素性证明和大数分解算法；第三部分为椭圆曲线公钥密码的有效实现，重点论述椭圆曲线公钥密码体制中的关键算子；标量乘法和双标量乘法的快速实现.

本书可以作为信息安全和密码学专业研究生的教材，也可供相关的研究人员参考.

图书在版编目(CIP)数据

椭圆曲线公钥密码导引/祝跃飞，张亚娟著. —北京：科学出版社，2006
(现代数学基础丛书；103)
ISBN 7-03-017360-0

I. 椭… II. ①祝… ②张… III. 密码–理论 IV. TN918.1

中国版本图书馆 CIP 数据核字(2006)第 057326 号

责任编辑：陈玉琢 贾瑞娜/责任校对：刘亚琦
责任印制：安春生/封面设计：王 浩

科 学 出 版 社 出版
北京东黄城根北街 16 号
邮政编码：100717
http://www.sciencep.com

源海印刷有限责任公司 印刷
科学出版社编务公司排版制作
科学出版社发行 各地新华书店经销

*

2006 年 10 月第 一 版 开本：B5 (720×1000)
2006 年 10 月第一次印刷 印张：16
印数：1—3 000 字数：298 000

定价：36.00 元

(如有印装质量问题，我社负责调换〈路通〉)

《现代数学基础丛书》序

对于数学研究与培养青年数学人才而言, 书籍与期刊起着特殊重要的作用. 许多成就卓越的数学家在青年时代都曾钻研或参考过一些优秀书籍, 从中汲取营养, 获得教益.

20 世纪 70 年代后期, 我国的数学研究与数学书刊的出版由于文化大革命的浩劫已经破坏与中断了十余年, 而在这期间国际上数学研究却在迅猛地发展着. 1978 年以后, 我国青年学子重新获得了学习、钻研与深造的机会. 当时他们的参考书籍大多还是 50 年代甚至更早期的著述. 据此, 科学出版社陆续推出了多套数学丛书, 其中《纯粹数学与应用数学专著》丛书与《现代数学基础丛书》更为突出, 前者出版约 40 卷, 后者则逾 80 卷. 它们质量甚高, 影响颇大, 对我国数学研究、交流与人才培养发挥了显著效用.

《现代数学基础丛书》的宗旨是面向大学数学专业的高年级学生、研究生以及青年学者, 针对一些重要的数学领域与研究方向, 作较系统的介绍. 既注意该领域的基础知识, 又反映其新发展, 力求深入浅出, 简明扼要, 注重创新.

近年来, 数学在各门科学、高新技术、经济、管理等方面取得了更加广泛与深入的应用, 还形成了一些交叉学科. 我们希望这套丛书的内容由基础数学拓展到应用数学、计算数学以及数学交叉学科的各个领域.

这套丛书得到了许多数学家长期的大力支持, 编辑人员也为其付出了艰辛的劳动. 它获得了广大读者的喜爱. 我们诚挚地希望大家更加关心与支持它的发展, 使它越办越好, 为我国数学研究与教育水平的进一步提高作出贡献.

杨　乐

2003 年 8 月

前　言

1985 年，V. Miller 和 N. Koblitz 各自独立地提出椭圆曲线公钥密码 (elliptic curves cryptography,ECC)，这是继 Goldwasser 和 Kilian 的素性检验， Lenstra 的椭圆曲线大数分解后，椭圆曲线理论在密码学中的又一次全新的应用. 它的思想仍然是在各种涉及有限域乘法群的公钥密码体制中，用有限域上的椭圆曲线构成的群来类比有限域的乘法群，从而获得类似的公钥密码体制. 这类体制的安全性是基于椭圆曲线上离散对数问题求解的困难性，目前还没有找到解决此问题的次(亚) 指数时间算法，因而它具有一些其他公钥密码体制无法比拟的优点，如在相同的安全强度下系统参数和密钥尺寸较短 (如 160bits 的 ECC 和 1024 bits 的 RSA 具有相当的安全强度)，选择余地较大等. 正是这些特点，十几年来，一直引起数学家、密码学家和计算机科学家们的极大关注，在理论和技术上获得大量成果的同时，许多国际标准化组织 (政府、工业界、金融界、商业界等) 已将各种椭圆曲线密码体制作为其标准化文件向全球颁布. ECC 标准大体可以分为两种形式：一类是技术标准，即描述以技术支撑为主的 ECC 体制，主要有 IEEEP 1363 、 ANSI X9.62 、 ANSI X9.63 、 SEC 1 、 SEC 2 、 FIP 186-2 及 ISO/IEC 14888-3. 规范了 ECC 的各种参数的选择，并给出了各级安全强度下的一组 ECC 参数. 另一类是应用标准，即在具体的应用环境中建议使用 ECC 技术，主要有 ISO/IEC 15946 、 IETFPKIX 、 IETF TLS 及 WAPWTLS 等. 在标准化的同时，一些基于标准 (或草案) 的各种椭圆曲线加密、签名、密钥交换的软、硬件也相继问世. 以加拿大 Certicom 为首的安全公司不仅和工业界联合共同研制、生产了以椭圆曲线密码算法为核心的密码产品，还提出了各种安全条件下对椭圆曲线离散对数攻击的悬赏挑战，这些举措大大刺激了 ECC 的理论和技术的发展. 目前，国外已开发出含 ECC 的密码引擎协处理器的 SIM 卡、Smart 卡，也研制出含 ECC 的高速 DSP 芯片和 FPGA 、ASIC 芯片. 在持续三年 (2000.01~2002.12) 的欧洲 NESSIE 工程中，及在日本电子政务的 CRYPTREC 工程中均有多个涉及 ECC 的候选方案. 可以相信，凭借其自身的优势， ECC 技术在信息安全领域中会发挥越来越大的作用.

椭圆曲线是一门古老而且内容丰富的数学分支，ECC 理论涉及了许多深奥的

椭圆曲线算术理论，要系统详细地讲授 ECC 理论需要有较深的数学基础. 本书的目的是在交换代数的基础之上系统阐述 ECC 理论，为有志于从事该方向研究的人员提供一本系统全面的基础性教材. 本书是专业教材，国内还没有这方面的教材，与国外同类书籍比较，本书内容丰富，有理论，有应用，有实践，且将最新的研究成果融入其中；书中所有的结果尽可能自包含，以形成一个完整的体系；丰富的内容使得本书的阅读面较广，除代数、数论专业以及密码学的研究生和相关专业的研究人员外，第三部分的实践所涉及的算法，也可供信息安全方面的工程人员参考.

本书围绕着 ECC 的理论和实践分三部分内容撰写. 第一部分 (第 1 、2 章) 为椭圆曲线基础. 介绍了椭圆曲线的算术理论，主要是有限域上椭圆曲线的相关理论；第二部分 (第 3~6 章) 为 ECC 的密码理论，重点论述了有限域上椭圆曲线的求阶算法，椭圆曲线上的离散对数求解算法和椭圆曲线公钥密码体制，椭圆曲线的素性证明和大数分解算法；第三部分 (第 7 章) 为椭圆曲线公钥密码的有效实现，重点论述椭圆曲线公钥密码体制中的关键算子: 包括标量乘法和双标量乘法的快速实现. 书中的大部分内容曾多次在解放军信息工程大学作为硕士研究生教材使用.

本书的编写和出版得到国家 973 项目 (编号: G1999035804) 、国家自然科学基金项目 (编号: 60473021) 的资助，特此感谢！

作　者

目　录

第 1 章 椭圆曲线

1.1 概 述

公元 250 年，古希腊的亚历山大 (Alexandia) 时代，出版了丢番图 (Diophantus [①]) 的巨作《算术》 (Arithmatic, 共 13 卷). 该书在历史上首次引入代数、方程、负数，后几卷涉及了数论的内容. 不幸的是，它出版后没过多久就被遗失了. 一千多年后，直到 1570 年才找到几卷，现保存的只有 6 卷. 尽管丢失了这么长时间，但该书中的许多工作并没有被重新发展. 书中所考虑的基本问题是有理多项式是否有有理解的问题，此问题分成以下两种形式.

(1) 仿射 (affine)：问 $f(x,y)\in\mathbb{Q}[x,y]$ 有无有理数解. 显然，通过乘以一个整数，便可以去掉 $f(x,y)$ 系数的分母，从而使得 $f(x,y)\in\mathbb{Z}[x,y]$，则问题转化为 $f(x,y)\in\mathbb{Z}[x,y]$ 有无有理数解.

(2) 投射 (projective)：问齐次方程 $f(x,y,z)\in\mathbb{Q}[x,y,z]$ 有无有理数解，即是否存在 $(0,0,0)\neq(x,y,z)\in\mathbb{Q}^3$ 满足 $f(x,y,z)=0$. 因为对于任意的 $t\in\mathbb{Q}$ 有 $f(tx,ty,tz)=t^{\deg f}f(x,y,z)$，即若 (x,y,z) 是所求的解，则 (tx,ty,tz) 也是解，称 (x,y,z) 和 (tx,ty,tz) 是等价的，则该等价类中一定有 $\mathbb{Z}^3$ 中的元素；又因为乘以一个整数不会改变方程的解，所以只需考虑整系数齐次多项式 $f(x,y,z)$ 有无整数解的问题.

进一步，若上述问题有解，考虑所有的解是否能用参数化表示的问题. 为了

---

① Diophantus：生活于公元 250 年前后的古希腊. 对于丢番图的生平事迹，人们知之甚少. 但在一本《希腊诗文选》中，收录了他的墓志铭：坟中安葬着丢番图，多么令人惊讶，它忠实地记录了他所经历的道路. 上帝给予的童年占 1/6，又过 1/12，两颊长髯，再过 1/7，点燃起结婚的蜡烛. 五年之后天赐贵子，可怜迟到的宁馨儿，享年仅及其父之半，便进入冰冷的墓. 悲伤只能用数论的研究去弥补，又过四年，他也走完了人生的旅途. 由此知道丢番图享年 84 岁. 他有几本著作，最重要的是《算术》，还有一部《多角数》，另一些已遗失. 《算术》是一部划时代的著作，虽然其是讲数论的，但是它引入了未知数，并对未知数加以运算，故可将其划归为代数. 丢番图把代数解放出来，摆脱了几何的羁绊，他认为代数方法比几何的演绎陈述更适宜于解决问题，而在解题的过程中显示出的高度技巧和独创性，在希腊数学中独树一帜. 他被后人称为“代数学之父”.

纪念丢番图，上述问题通称为丢番图问题，所涉及的不定方程称为丢番图方程.

注意到，仿射和投射是可以互相转化的. 例如，考虑仿射方程 $u^n + v^n = 1$ 是否有有理解的问题，通过变量代换

$$u \leftarrow \frac{x}{z}, v \leftarrow \frac{y}{z},$$

该问题转化为投射方程 $x^n + y^n = z^n$ 是否有非平凡的整数解 (即 $z \neq 0$) 的问题，当 $n = 2$ 时，见习题 1.1；当 $n \geqslant 3$ 时，该问题即是著名的费马 (Fermat ①) 问题. 1993 年，安得鲁 · 怀尔斯 (A.Wiles ②) 用椭圆曲线等相关现代数学理论证明了费马大定理.

以下从一些简单的投射丢番图方程入手，考虑丢番图问题.

(1) 一次的投射丢番图方程为投射线 $ax + by + cz = 0$， $a, b, c \in \mathbb{Z}$ 不同时为 0. 其在 $\mathbb{Z}^3$ 的解是容易求得的，且所有的解可以参数化表示.

(2) 二次的投射丢番图方程，通过合适的线性变换，不妨设为 $ax^2 + by^2 + cz^2 = 0$， $a, b, c \in \mathbb{Z}$ 不同时为 0. 对该方程无解的判断相对来说容易得多，举例如下.

① $x^2 + y^2 + z^2 = 0$ 无平凡整数解：因为平方数均不小于 0，即在 $\mathbb{R}$ 中无解.

② $x^2 + y^2 = 3z^2$ 无平凡整数解：因为任意整数解均可以诱导出一组互素的整数解，所以不妨设该方程有互素的整数解 $x, y, z \in \mathbb{Z}$, 则方程两边同时模 3，可得 $x^2 + y^2 \equiv 0 \mod 3$，显然 3 一定是 x, y, z 的公因子，矛盾.

---

①费马 (1601.8~1665.1), 法国数学家，生于图卢兹 (Toulouse) 附近的一个皮革商人家庭，他学习过法律并担任过律师，业余研究数学. 他受到由法国数学家 Bachet 翻译成拉丁文的丢番图《算术》 (1621 年出版) 的影响，潜心研究数论，在看到毕达哥拉斯 (Pythagoras) 问题的章节时，他写道“ $n \geqslant 3$ 时， $x^n + y^n = z^n$ 无平凡整数解，我已获得一个巧妙的证明方法，但由于书的空隙太小无法写下来”.

②怀尔斯 (1953~),1953 年 4 月 11 日生于英国剑桥. 1971 年入牛津大学莫顿 (Merton) 学院学习， 1974 年获该校学士学位. 同年入剑桥大学柯雷尔 (Clare) 学院学习， 1980 年获该校博士学位. 1977~1980 年，是柯雷尔学院的“青年研究会员”和哈佛大学的“本杰明 · 裴尔斯助教授”. 1981 年是波恩的“理论数学专门研究院”访问教授，此年稍后，为美国普林斯顿的“高等研究所”研究员. 1982 年成为普林斯顿大学教授，该年春是奥赛的巴黎大学访问教授. 作为古根海特别研究员，他在 1985~1986 年是科学高级研究所 (IHES) 和高级师范学校 (ENS) 的访问教授. 1988~1990 年是牛津大学皇家学会研究教授. 1994 年，他取得现在的普林斯顿大学欧根 · 黑金斯数学教授职位. 怀尔斯于 1989 年被选为在伦敦的皇家学会研究员. 1995 年获瑞典皇家科学院的数学韶克奖. 同年获费马奖，由保罗萨巴提尔大学和马特拉马克尼空间颁发. 1996 年获沃尔夫奖和 (美国) 国家科学院奖.

若丢番图方程有整数解，显然在实数域 $\mathbb{R}$ 中有解，在任意 p-adic 整环 $\mathbb{Z}_p$(或 p-adic 数域 $\mathbb{Q}_p$) 中有解. 反之是否成立呢？ Hasse ① 对此给出了正式的归纳：若一个齐次方程在 $\mathbb{Q}$ 上有解当且仅当它在 $\mathbb{R}$ 和任意 $\mathbb{Q}_p$ 上有解，简述成整体有解当且仅当局部有解. 该命题称作局部整体原则 (local global principle)，由于 Hasse 是在 Minkowski ② 已证明了对二次齐次方程局部整体原则是正确的基础上提出的，故又称之为 Hasse-Minkowski 原理. 利用局部整体原则，判别丢番图方程无整数解比有整数解要容易. Hensel ③ 证明了 $\mathbb{Q}_p$ 上的求解问题可以转化为 $\mathbb{F}_p$ 上的求解问题，所以丢番图方程求整数解的问题转化为在 $\mathbb{R}$ 和 $\mathbb{F}_p$ 中求解问题，其中 p 是所有的素数.

(3) 三次投射丢番图方程没有一个一致的结果. 1951 年， Selmer 证明了方程 $3x^3+4y^3+5z^3=0$ 局部有解，但整体无解. 所以当方程次数为 3 时，局部整体原则不成立. 继续考虑下面几个三次方程的例子.

①三次 Fermat 方程 $x^3+y^3=z^3$：对其作变量代换为

$$\begin{cases} \dfrac{x}{z}=\dfrac{3u}{v} \\ \dfrac{y}{z}=\dfrac{v-9}{v} \end{cases}$$

则得 $v^2-9v=u^3-27$.

②同余 (congruent) 数问题： $r\in\mathbb{Q}$ 称作同余数，若 r 是一个有理数边构成的直角三角形的面积，即

$$r\text{是同余数} \Longleftrightarrow \text{存在 } x,y,z\in\mathbb{Q}\text{使得} \begin{cases} x^2+y^2=z^2 \\ r=\dfrac{1}{2}xy \end{cases}$$

同余数问题是指是否存在同余数. 如果 r 是同余数，则对于任意的 $s\in\mathbb{Q}$，

---

① Hasse (1898~1979)，德国哥廷根大学教授，师从 Hensel，在类域论、复乘等方面有过杰出的成果.

② Minkowski(1864~1909)，德国哥廷根大学教授，在二次型、连分式等方面有过杰出的成果.

③ Hensel(1861~1941)，德国 Marburg 大学教授，师从 Weierstrass、Kirchhoff、Helmholtz 和 Kronecker，主要研究领域是代数数域.

均有 s^2r 是同余数，故同余数问题只需考虑无平方因子整数 r. 由方程

$$\begin{cases} x^2+y^2=z^2 \\ r=\dfrac{1}{2}xy \end{cases}$$

可得 $(x\pm y)^2=z^2\pm 4r$, $\left(\dfrac{x\pm y}{2}\right)^2=\left(\dfrac{z}{2}\right)^2\pm r$, 则 $\left(\dfrac{x^2-y^2}{4}\right)^2=\left(\dfrac{z}{2}\right)^4-r^2$, 令 $u=\dfrac{z}{2}, v=\dfrac{x^2-y^2}{4}$ ，有 $v^2=u^4-r^2, u^6-r^2u^2=(uv)^2$, 再令 $u^2=x, uv=y$, 可得 $x^3-r^2x=y^2$. 因此，若 $x^3-r^2xz^2=y^2z$ 在 $\mathbb{Q}$ 中有 $z\neq 0$ 的解，则 $y^2=x^3-r^2x$ 在 $\mathbb{Q}$ 中有解，从而

$$\begin{cases} x^2+y^2=z^2 \\ r=\dfrac{1}{2}xy \end{cases}$$

在 $\mathbb{Q}$ 中有解.

③对于给定的数，如 6 ，是否能将其分成两部分 (有理数) ，使它们的乘积是一个数的立方和此数的差，即

$$6y-y^2=x^3-x$$

是否有有理数解？ $P=(x,y)=(-1,0)$ 是方程的一个解，考虑过 P 点的所有直线与上述方程的交点. 设直线为 $x=2y-1$ ，代入方程得

$$6y-y^2=8y^3-12y^2+6y-1-2y+1=8y^3-12y^2+4y,$$

显然 $y\neq 0$ 在 $\mathbb{R}$ 中无解. 即除了 P 点外，该直线和方程在实平面内没有其他的交点. 设直线为 $x=3y-1$ ，代入方程得

$$6y-y^2=27y^3-27y^2+6y,$$

故 $y=\dfrac{26}{27}, x=\dfrac{17}{9}$ 是直线与方程的交点，即其为方程的解.

④ Bacht 问题：考虑一个有理数 c 如何写成一个平方 (有理) 数和一个立方 (有理) 数之差. 即可描述成 Bacht 方程： $y^2-x^3=c$ 是否有有理数解？ 1621 年， Bacht 证明了若 (x,y) 是一个解，则

$$\left(\frac{x^4-8cx}{4y^2}, \frac{-x^6-20cx^3+8c^2}{8y^3}\right)$$

也是一个解. 令人惊讶的是 Bacht 如何找到这样的非平凡的解呢？后人用③中所述的直线和方程相交的思想给出了解释. 然而，要知道笛卡儿[①]在 1637 年出版《几何学》，才引入坐标系、用符号代数来研究轨迹等几何问题，而 Bacht 生活在笛卡儿之前，难道那时 Bacht 的思维里已有坐标系的概念了吗？

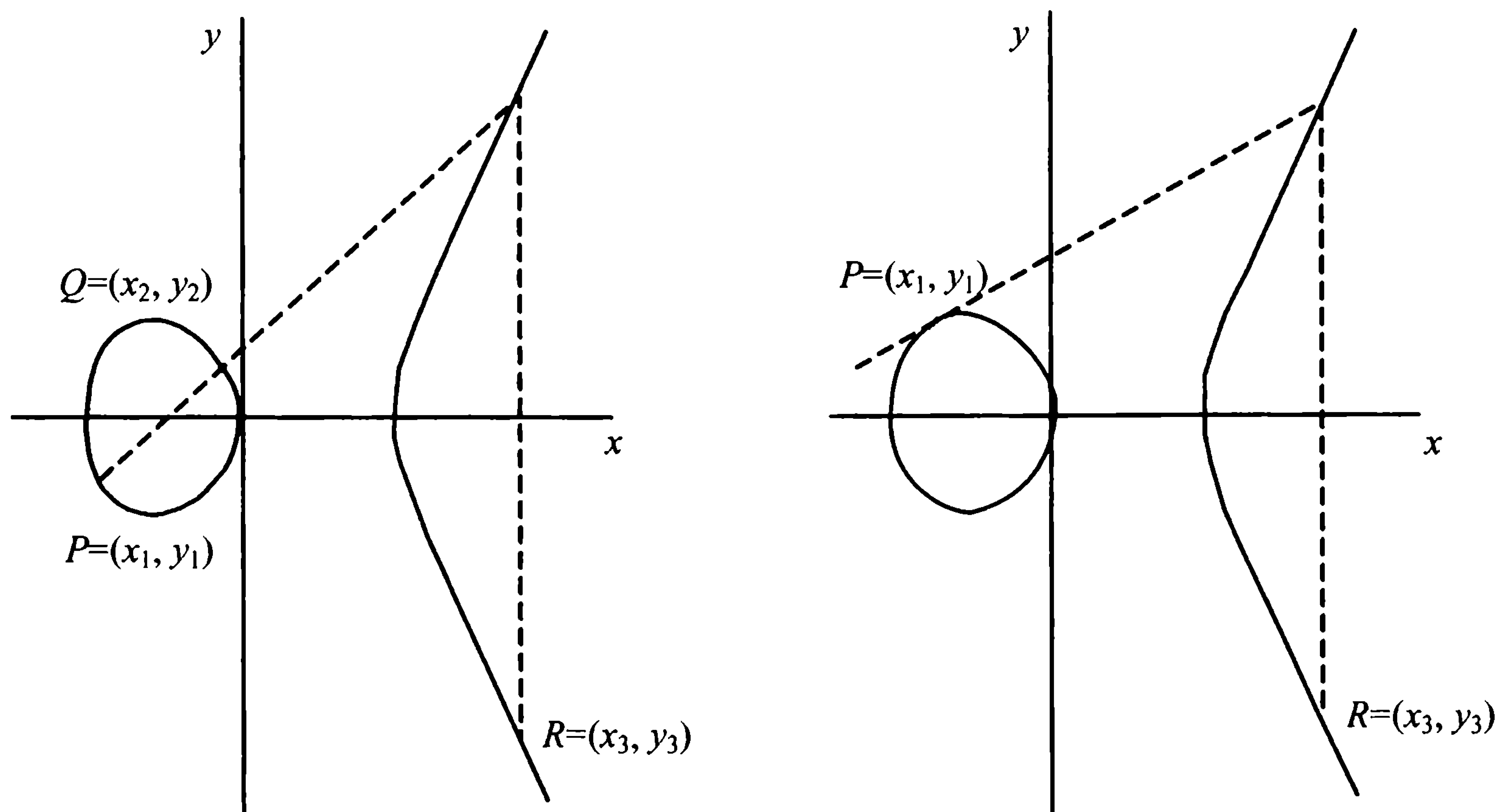
上述四个例子均可归结为一类三次方程，即所谓的 Weierstrass 方程

$$y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6,\qquad a_i\in\mathbb{Q}.$$

光滑的 Weierstrass 方程所确定的曲线加上一个特定点 O (无穷远点) 称为 $\mathbb{Q}$ 上的椭圆曲线. 同样，可定义 $\mathbb{R},\mathbb{C},\mathbb{Q}_p,\mathbb{F}_p$ 上的椭圆曲线，如

$$E(\mathbb{R})=\{(x,y)\in\mathbb{R}^2:y^2+a_1xy+a_3y=x^3+a_2x^2+a_4x+a_6\}\cup\{O\}$$

从几何角度利用弦切法可以在 $E(\mathbb{R})$ 上定义“ + ”运算: 对于椭圆曲线上的点 P,Q，过点 P,Q 的直线 (若 $P=Q$ ，则取过点 P 的切线) 和椭圆曲线必有第三个交点 (考虑重数)，过该点和 O 的直线与椭圆曲线的另一交点即定义为 $P+Q$. 如图 1.1 所示.



弦切法:　$R=P+Q$　　$R=P+P=2P$

图 1.1　弦切法示意

①笛卡儿 (Descart,1596~1650)，生于法国土伦省莱耳市的一个贵族之家，卒于斯德哥尔摩. 1612 年在普瓦捷大学攻读法学，四年后获博士学位; 1628 年移居荷兰; 1637 年发表的《几何学》标志着解析几何学的诞生，确定了其在数学史上的地位; 1649 年到斯德哥尔摩任宫廷哲学家，为瑞典女王授课; 其在数学、物理及哲学等众多领域都有杰出贡献，堪称 17 世纪及其后的欧洲哲学界和科学界最有影响的巨匠之一，被誉为“近代科学的始祖”.

则 $(E(\mathbb{R}),+)$ 构成群 (Poincaré [①] 定理),$(E(\mathbb{Q}),+)$ 是其子群. 对于域 K 上 Weierstrass 方程的解确定的椭圆曲线 $E(K)$, 虽然没有几何图像直观表示, 但利用弦切法所决定的代数公式, 自然可以定义 $E(K)$ 上的加法, 使其构成一个加法群. 本书重点论述 K 为有限域 $\mathbb{F}_q$ 的情况. 一方面从前面论述已知, 判断 E 有无非有理数解, 根据局部整体原则和 Hensel 引理, 需要研究 $E(\mathbb{Q}_p)$, $E(\mathbb{R})$, $E(\mathbb{C})$, $E(\mathbb{F}_q)$ 的结构和相关性质及理论. 另一方面, 椭圆曲线能够在密码中应用的关键是椭圆曲线的群结构, 由于密码系统是个离散的系统, 它需要用有限群来构筑系统的基础, 因此 $E(\mathbb{F}_q)$ 的结构和性质是本书的讲述重点. 若没有特殊声明, $\mathbb{Z}_n$ 均表示商群 $\mathbb{Z}/n\mathbb{Z}$.

定理 1.1.1 (Poincaré 定理) $(E(\mathbb{F}_q),+)$ 是一个阿贝尔群.

定理 1.1.2 (Hasse 定理) $|E(\mathbb{F}_q)| = 1 + q - t$, 其中 t 满足 $|t| \leqslant 2\sqrt{q}$.

定理 1.1.3 (群结构) $E(\mathbb{F}_q) \cong \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$, 其中 $n_1|n_2, n_1|q-1$.

1.2 仿射平面曲线

本章用 K 表示代数闭域. 本节介绍了仿射曲线的概念及基本性质.

定义 1.2.1 集合 $K \times K$ 称为 K 上的仿射平面 (affine plane) , 记作 $A^2(K)$.

定义 1.2.2 K 上的一条仿射曲线是指 $K[X,Y]$ 中一个不可约多项式 C 的零点集, 即 $C(K) = \{(a,b) \in A^2(K) : C(a,b) = 0\}$.

若给定 K 上的不可约多项式 C 也可看作 K 的某个子集 k 上的多项式, 即 $C \in k[X,Y]$, 则以后常称仿射曲线 $C(K)$ 的子集 $C(k) = \{(a,b) \in k^2 : C(a,b) = 0\}$ 为 C 在 k 上的有理点集.

例 1.1 令 $k = \mathbb{R}, K = \mathbb{C}$, 曲线 D, E, F 在 $\mathbb{R}$ 上的有理点集的构成如图 1.2 所示.

因为 K 是代数闭域, 所以任意曲线均有无限多个点: 对于任意 $x \in K$, 方程 $C(x,Y)$ 在 K 中至少有一个解, 记作 y , 则 $P = (x,y)$ 是曲线上的点. 为描述方便起见, 以下将曲线和不可约多项式不加区别 (参见习题 1.2) , 常称 C 是一条曲线或曲线 C , 在不引起混淆的情况下, 曲线可简记为 C.

---

① Poincaré(1854~1912), 生于法国南锡 (Nancy) , 1879 年在巴黎大学获数学博士学位, 同年任教于 Caen 大学, 1887 年当选为法国科学院 (the Académie des Sciences) 院士, 1906 年成为科学院主席, 在数学分析、代数、拓扑、应用数学等领域均有杰出贡献.

$D: \ Y^2-(X^3+X^2)$ $\qquad E: \ Y^2-(X^3-X)$ $\qquad F: \ Y^2-X^3$

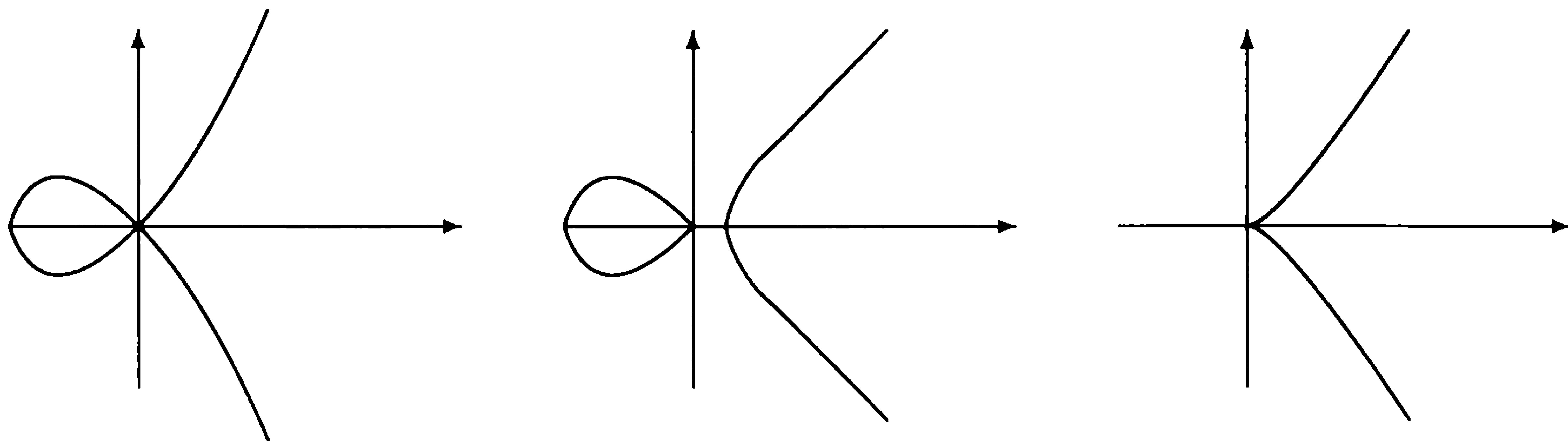


图 1.2 例 1.1 图

定义 1.2.3 设 C 是一条曲线，$P=(a,b)$ 是 C 上一个点. 若 $\frac{\partial C}{\partial X}|_{(a,b)}=\frac{\partial C}{\partial Y}|_{(a,b)}=0$，则称 P 是 C 上奇异点. 否则，称 P 是 C 上的非奇异点或光滑点，且称 $\frac{\partial C}{\partial X}|_P(X-a)+\frac{\partial C}{\partial Y}|_P(Y-b)=0$ 为 C 在 P 点的切线. 一条含有奇异点的曲线称为奇异曲线，否则称为非奇异曲线或光滑曲线.

例 1.2 仿射曲线 D、E、F 同例 1.1.

(1) 因为

$$\begin{aligned}\frac{\partial D}{\partial X}(0,0)=\frac{\partial D}{\partial Y} &= 0,\\ \frac{\partial F}{\partial X}(0,0)=\frac{\partial F}{\partial Y} &= 0.\end{aligned}$$

所以 $(0,0)$ 是 D 和 F 上的奇异点.

(2) 因为

$$\frac{\partial E}{\partial X}(0,0)=(-3X^2+1)|_{X=0}=1\neq 0,$$

所以 $(0,0)$ 是 E 上的非奇异点.

将 $C(X,Y)$ 在 $P=(a,b)$ 点展开，一定有形式

$$C(X,Y)=\frac{\partial C}{\partial X}|_P(X-a)+\frac{\partial C}{\partial Y}|_P(Y-b)+\text{高次项},$$

所以可以知道，$C(X,Y)$ 在 $P=(a,b)$ 奇异当且仅当上式没有一次项，否则一次项就是在 P 点的切线.

在代数闭域上，一个二次项一定能写成两个一次项的乘积，即

$$\begin{aligned}&\alpha(X-a)^2+\beta(X-a)(Y-b)+\gamma(Y-b)^2\\ &=(\alpha_1(X-a)+\beta_1(Y-b))(\alpha_2(X-a)+\beta_2(Y-b)),\end{aligned}$$

设 P 是奇异点，若 $\alpha_1(X-a)+\beta_1(Y-b)=\alpha_2(X-a)+\beta_2(Y-b)$, 称 P 为尖点 (cusp)，否则称为叉点 (node). 例如，曲线 D 在 $(0,0)$ 点有 2 条切线，$Y=\pm X$，故 $(0,0)$ 是叉点；曲线 E 在 $(0,0)$ 点有一条二重的切线 $X=0$，故 $(0,0)$ 是尖点.

对于 $g(X,Y)\in K[X,Y]$，可以如下定义 C 到 K 的映射，即

$$g(X,Y):\quad \begin{cases} C \longrightarrow K \\ (a,b)\mapsto g(a,b) \end{cases}$$

该映射常称为多项式映射. 显然对于多项式 $f(X,Y)$,$g(X,Y)\in K[X,Y]$，其作为多项式映射相等当且仅当 $C|f-g$.

定义 1.2.4 曲线 C 上的多项式环为 $K[C]=K[X,Y]/(C)$，即是全体多项式映射构成的集合.

为描述方便，以下将 X,Y 在 $K[C]$ 中的剩余类仍记作 X,Y，其真正的含义可从上下文得知. 因为 C 不可约，所以 $K[C]$ 是整环.

定义 1.2.5 $K[C]$ 的分式域称为 C 上的有理函数域，记作 $K(C)$.

定义 1.2.6 设有理函数 $r\in K(C),P\in C$，若存在 $f,g\in K[C]$, 使得 $r=\dfrac{f}{g}$ 且 $g(P)\neq 0$，则称 r 在 P 点正则 (regular)，记 $r(P)=\dfrac{f(P)}{g(P)}$；在 P 点正则的有理函数的全体构成环，称为 C 在 P 的局部环，记作 $O_P(C)$. 若 r 在 P 点不正则，常记作 $r(P)=\infty$.

所有在 P 点正则的有理函数在 P 点的取值是与有理函数的表示无关的：假设

$$r=\frac{f_1}{g_1}=\frac{f_2}{g_2},$$

其中，$f_1,g_1,f_2,g_2\in K[C],g_1(P)\neq 0,g_2(P)\neq 0$，则在 $K[C]$ 中有

$$f_1g_2=f_2g_1,$$

所以存在 $h\in K[X,Y]$，使得在 $K[X,Y]$ 中有

$$f_1g_2-f_2g_1=hC,$$

因此

$$f_1(P)g_2(P)-f_2(P)g_1(P)=h(P)C(P)=0,$$

即

$$\frac{f_1(P)}{g_1(P)} = \frac{f_2(P)}{g_2(P)}.$$

显然 $O_P(C)$ 是环，进一步可证是局部环，其中的单位，即可逆元构成的集合为

$$O_P(C)^\times = \{r \in O_P(C) : r(P) \neq 0\},$$

其唯一的极大理想为

$$M_P(C) = \{r \in O_P(C) : r(P) = 0\}.$$

可以证明， $K(C)$ 是以 K 为常值域的单变量代数函数域 (见习题 1.3).

例 1.3 考虑例 1.1 中的曲线 $E : Y^2 = X^3 - X, P = (0,0)$, $r = \dfrac{X}{Y} \in K(E), s = \dfrac{1}{r}$, 那么

$$r = \frac{XY}{Y^2} = \frac{Y}{X^2-1},$$

则 $r(P) = 0$, 即 r 在 P 点正则；假设 s 在 P 点正则，那么

$$0 = s(P)r(P) = 1(P) = 1,$$

矛盾，故 s 在 P 点不正则.

定理 1.2.7 设 C 是一条曲线， $P = (a,b) \in C$ ，则 $K[C]$ 是一维诺特整环；其极大理想均为 $\wp = (X-a, Y-b)$ ， $O_P(C) = K[C]_\wp$ ；且 $O_P(C)$ 是离散赋值环当且仅当 P 是 C 的非奇异点，其中 $K[C]_\wp$ 是 $K[C]$ 对于 $\wp$ 的局部化.

证明 因为 $K[X,Y]$ 是二维诺特环，所以 $K[C]$ 是一维诺特的. 又因为 C 不可约，所以 $K[C]$ 是整环. 而 $K[X,Y]$ 的极大理想均为 $(X-s, Y-t), s, t \in K$ ，所以 $K[C]$ 的极大理想为

$$\frac{(X-a, Y-b)}{(C)},$$

其中， (a,b) 满足 $C(a,b) = 0$. 故 C 上的点与 $K[C]$ 的极大理想一一对应. 对于 $\wp = (X-a, Y-b)$ ，有

$$\begin{aligned} K[C]_\wp &= \left\{\frac{g}{h} : g, h \in K[C], h \notin \wp\right\} \\ &= \left\{\frac{g}{h} : g, h \in K[C], h(a,b) \neq 0\right\} \\ &= O_P(C). \end{aligned}$$

因为 $K[C]$ 是一维诺特的，所以 $O_P(C)=K[C]_\wp$ 也是一维诺特整环，则 $O_P(C)$ 是离散赋值环当且仅当 $O_P(C)$ 是整闭的，当且仅当 $O_P(C)$ 是主理想整环.

设 $P=(a,b)$ 是 C 的非奇异点，要证明 $O_P(C)$ 是主理想整环，由习题 1.5 的结论和 $O_P(C)$ 是一维诺特整环，可知只需证所有的极大理想均为主理想即可. 又因为 $O_P(C)$ 是局部环，$O_P(C)$ 的极大理想为

$$M_P=\left\{\frac{g}{h}:h(a,b)\neq 0,g(a,b)=0\right\}.$$

不妨设 $(a,b)=(0,0)$，则 $M_P=(X,Y)$. 因为 C 在 P 点非奇异，所以不妨设 $\frac{\partial C}{\partial Y}|_P=\delta\neq 0$，$C$ 在 P 点的泰勒 (Tayler) 展开式为

$$C(X,Y)=\frac{\partial C}{\partial X}|_P X+\frac{\partial C}{\partial Y}|_P Y+\cdots=\sum_{i=1}^{n}b_iX^i+Y(\delta+g(X,Y)),$$

其中，$b_i\in K,g(X,Y)\in K[X,Y],g(0,0)=0$，因为在 $K[C]$ 中 $C(X,Y)=0$，所以在 $K[C]$ 中有

$$-\sum_{i=1}^{n}b_iX^i=Y(\delta+g(X,Y)),$$

而 $\delta\neq 0$，$K[C]_P$ 的极大理想为 (X,Y)，故 $\delta+g(X,Y)\notin M_P$，即其是 $K[C]_P$ 的可逆元，所以在 $K[C]_P$ 中 Y 可由 X 表示出，即 $(X,Y)=(X)$.

设 $O_P(C)$ 是主理想整环，要证明 $P=(a,b)$ 是非奇异点. 不妨设 $(a,b)=(0,0)$，则 $O_P(C)$ 的极大理想为 $M_P=(X,Y)$，因为 M_P 是主理想，即存在 $Z\in K[C]_P$，使得 $(Z)=(X,Y)$，则存在 $s,r,u,v\in K[C]_P$，使得 $X=Zs,Y=Zr,Z=Xu+Yv$，所以 $su+rv=1$. 若 s,r 均不可逆，则 $1\in M_P$，矛盾，故 s,r 中必有一个可逆，不妨设 s 可逆，则得 $Y=\frac{r}{s}X$，所以存在 $\hat{r},\hat{s}\in K[C],\hat{s}(0,0)\neq 0$，使得 $Y=\frac{\hat{r}}{\hat{s}}X$，进而存在 $\tilde{s},\tilde{r}\in K[X,Y],\tilde{s}(0,0)\neq 0$，使得 $\tilde{s}Y-\tilde{r}X=Cg$，利用 C 在 P 点的泰勒展式并比较 Y 的系数可得

$$\tilde{s}(0,0)=\frac{\partial C}{\partial Y}|_P g(0,0),$$

所以 $\frac{\partial C}{\partial Y}|_P\neq 0$，即 P 是非奇异点. 结论得证.

因为 $K[C]$ 是一维诺特整环，所以 $K[C]$ 整闭当且仅当 $K[C]$ 是戴德金(Dedekind) 整环，当且仅当 $K[C]$ 对所有的素理想 $\wp$ 局部化所得的 $K[C]_\wp$ 为离散赋值环，再利用上述定理易得以下推论:

推论 1.2.8 设 C 是一条曲线，则 $K[C]$ 是戴德金整环当且仅当 C 是光滑曲线.

1.3 仿射 Weierstrass 方程

本节将介绍仿射椭圆曲线，研究其相应的多项式环及有理函数域.

定义 1.3.1 方程 $E: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, a_i \in K, i = 1,2,3,4,6$ 称为仿射 Weierstrass 方程. 定义如下与 E 相关的变量:

$$
\begin{aligned}
b_2 &= a_1^2 + 4a_2,\\
b_4 &= 2a_4 + a_1a_3,\\
b_6 &= a_3^2 + 4a_6,\\
b_8 &= a_1^2a_6 + 4a_2a_6 - a_1a_3a_4 + a_2a_3^2 - a_4^2,\\
c_4 &= b_2^2 - 24b_4,\\
c_6 &= b_2^3 + 36b_2b_4 - 216b_6,\\
\Delta &= -b_2^2b_8 - 8b_4^3 - 27b_6^2 + 9b_2b_4b_6,\\
j &= \frac{c_4^3}{\Delta}, \qquad \text{若}\Delta \neq 0.
\end{aligned}
$$

Δ 称为 E 的判别式；j 称为 E 的不变量. 非奇异的 Weierstrass 方程定义的曲线为仿射椭圆曲线.

定理 1.3.2 E 在 $K[X,Y]$ 中是不可约的.

证明 易证 E 在 $K[X,Y]$ 中不可约当且仅当在 $K(X)[Y]$ 中不可约 (见习题 1.6). 假设 E 在 $K[X,Y]$ 中可约，即 $E=(Y+s)(Y+r), r,s \in K(X)$，则

$$
\begin{aligned}
r + s &= a_1X + a_3,\\
rs &= -(X^3 + a_2X^2 + a_4X + a_6).
\end{aligned}
$$

对于 $f, g \in K[X]$，定义

$$
\begin{aligned}
\deg \frac{f}{g} &= \deg f - \deg g,\\
\deg(fg) &= \deg f + \deg g,
\end{aligned}
$$

则

$$\deg(f+g) \leqslant \max\{\deg f, \deg g\}, \text{且当} \deg f \neq \deg g \text{等号成立},$$

故 $1 \geqslant \deg(r+s) = \max\{\deg r, \deg s\} \geqslant \frac{3}{2}$ 矛盾，所以 E 在 $K[X,Y]$ 不可约.

因为 E 不可约，所以 E 是曲线. 显然 $K[X]$ 是 $K[E]$ 的子环， $K(X)$ 是 $K(E)$ 的子域，令 $L = K(X)[Y]/(E)$ ，因为 E 不可约，所以 L 是 $K(X)$ 的二次扩张. 又因为 $K[E] \subseteq L$ ，故 $L = K(E)$ ，因此 $K(E)$ 是 $K(X)$ 的二次扩张，从而是 Galois 扩张. 令 $\mathrm{Gal}(K(E)/K(X)) = \{1, \sigma\}$ ，以后常记 $\sigma(f)$ 为 $\bar{f}$ ，称 σ 为 $K(E)$ 的共轭映射，则 $\bar{f}(X,Y) = f(X,\bar{Y})$. 对于 $P = (x,y) \in E$ ，令 $\bar{P} = (x,\bar{y}) \in E$ ，那么 $\bar{f}(P) = f(\bar{P})$.

用 N,Tr 分别表示 $K(E)$ 到 $K(X)$ 的范数和迹，即

$$\begin{aligned} N : K(E) &\to K(X), \\ f &\mapsto f\,\bar{f}; \\ \mathrm{Tr} : K(E) &\to K(X), \\ f &\mapsto f + \bar{f}. \end{aligned}$$

直接计算可得.

例1.4 $N(X) = X^2$;

$$N(Y) = Y(-Y - a_1X - a_3) = -(X^3 + a_2X^2 + a_4X + a_6);$$

$$\mathrm{Tr}(X) = 2X;$$

$$\mathrm{Tr}(Y) = -(a_1X + a_3).$$

若 $f \in K(E)$ 表示成 $f = u + vY, u, v \in K(X)$, 则有

$$N(f) = (u + vY)(u + v\bar{Y}) = u^2 + \mathrm{Tr}(Y)uv + N(Y)v^2;$$

$$\mathrm{Tr}(f) = (u + vY) + (u + v\bar{Y}) = 2u + v\mathrm{Tr}(Y).$$

下面考虑不改变 Weierstrass 方程形式的可逆仿射变换. 设 Weierstrass 方程

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6, \quad a_i \in K$$

通过可逆仿射变换

$$\psi : \begin{pmatrix} X \\ Y \end{pmatrix} \longleftarrow \begin{pmatrix} a & b \\ c & d \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} + \begin{pmatrix} r \\ t \end{pmatrix}$$

即

$$\psi : \begin{cases} X \leftarrow aX + bY + r \\ Y \leftarrow cX + dY + t \end{cases}$$

作用得 Weierstrass 方程 $E' : Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6'$ ，则除了要求

$$\begin{pmatrix} a\ b \\ c\ d \end{pmatrix}$$

可逆外，还可得出：

(1) $a^3 = d^2, a \neq 0$, 令 $a = u^2$ 则 $d = u^3$.

(2) 因为 Y^3 不出现，所以 $b = 0$.

即为了保证 Weierstrass 方程形式不变，仿射变换 ψ 的形式为

$$\begin{cases} X \leftarrow u^2X + r \\ Y \leftarrow u^3Y + u^2sX + t \end{cases} \tag{1.1}$$

其中，$u \in K^{\times}, r, s, t \in K$, 将这种仿射变换称为允许变换 (admissable change).

定义 1.3.3 称 Weierstrass 方程决定的曲线

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

$$E' : Y^2 + a_1'XY + a_3'Y = X^3 + a_2'X^2 + a_4'X + a_6'$$

是同构的 (isomorphic)，如果 E' 可由 E 通过允许变换获得.

例 1.5 仿射变换 $(X, Y) \leftarrow (X, -Y - a_1X - a_3)$ 是允许变换. 其中

$$\begin{cases} u^2 = 1 \\ u^3 = -1 \end{cases} \Rightarrow \begin{cases} u = -1, \\ r = 0, \\ s = -a_1, \\ t = -a_3. \end{cases}$$

上述定义的曲线的同构是等价关系. 令 $u = 1, r = s = t = 0$ ，则恒等变换是允许变换，所以同构具有反身性. 允许变换 ψ 的逆变换为

$$\psi^{-1} : \begin{pmatrix} X \\ Y \end{pmatrix} \leftarrow \begin{pmatrix} u^{-2} & 0 \\ -u^{-3}s & u^{-3} \end{pmatrix} \begin{pmatrix} X \\ Y \end{pmatrix} - \begin{pmatrix} u^{-2}r \\ u^{-3}(t - rs) \end{pmatrix}$$

显然是允许变换，所以同构具有对称性. 同构具有传递性请读者证明. 因而同构是一个等价关系.

在式 (1.1) 的允许变换下， E 和 E' 的系数间存在如下关系：

$$\begin{cases} a_1' = u^{-1}(a_1 + 2s), \\ a_3' = u^{-3}(a_3 + ra_1 + 2t), \\ a_2' = u^{-2}(a_2 - sa_1 + 3r - s^2), \\ a_4' = u^{-4}(a_4 + 2ra_2 - (rs + t)a_1 - sa_3 + 3r^2 - 2st), \\ a_6' = u^{-6}(a_6 + r^2 a_2 + ra_4 - rta_1 - ta_3 + r^3 - t^2), \\ b_2' = u^{-2}(b_2 + 12r), \\ b_4' = u^{-4}(b_4 + rb_2 + 6r^2), \\ b_6' = u^{-6}(b_6 + 2rb_4 + r^2 b_2 + 4r^3), \\ b_8' = u^{-8}(b_8 + 3rb_6 + 3r^2 b_4 + r^3 b_2 + 3r^4), \\ c_4' = u^{-4} c_4, \\ \Delta' = u^{-12}\Delta. \end{cases}$$

可知，在允许变换下 $j' = j$, 即同构曲线有相同的 j 不变量. 在代数闭域 K 上，其逆命题也成立，即 K 上具有相同 j 不变量的两条曲线同构. 若 Weierstrass 方程非奇异，则 j 有意义.

Weierstrass 方程 E 到 E' 的允许变换 ψ, 本质上给出了同构曲线间的一个双射：

$$\begin{aligned} \phi: \quad & E \to E', \quad (x, y) \mapsto (u^{-2}(x - r), u^{-3}(y - sx - t + rs)), \\ \phi': \quad & E' \to E, \quad (x, y) \mapsto (u^2 x + r, u^3 y + u^2 sx + t), \end{aligned}$$

$\phi' \circ \phi = \mathrm{id}|_E, \phi \circ \phi' = \mathrm{id}|_{E'}$ ，其中 id 表示恒等映射.

进一步， Weierstrass 方程 E 到 E' 的允许变换 ψ 可以自然地扩展为 $K[E]$ 到 $K[E']$ ， $K(E)$ 到 $K(E')$ 的同构，仍记为 ψ. 易知对于任意的 $P \in E$ ， ψ 也诱导了 $O_P(E)$ 到 $O_{\phi(P)}(E')$ 的同构.

因为 $\psi(K(X)) \subseteq K(X), \psi^{-1}(K(X)) \subseteq K(X)$ ，所以 ψ 也是 $K(X)$ 的自同构. 对于 $K(E)$ 的共轭映射 σ ，定义 $\sigma' = \psi \circ \sigma \circ \psi^{-1}$ ，则 σ' 是 $K(E')$ 的自同构，且保持 $K(X)$ 不动：

$$(\psi \circ \sigma \circ \psi^{-1})(f) = f$$

$$\begin{aligned}&\Leftrightarrow \sigma(\psi^{-1}(f)) = \psi^{-1}(f)\\&\Leftrightarrow \psi^{-1}(f) \in K(X)\\&\Leftrightarrow f \in \psi(K(X)) = K(X).\end{aligned}$$

因此 σ' 是 $K(E')$ 的共轭映射，则

$$\overline{\psi(f)} = (\sigma' \circ \psi)(f) = (\psi \circ \sigma)(f) = \psi(\overline{f}).$$

故 $N(\psi(f)) = \psi(N(f)), \mathrm{Tr}(\psi(f)) = \psi(\mathrm{Tr}(f))$.

由以上可知，研究局部环 $O_P(E)$ 、共轭映射、迹函数、范数等性质，仅需对 E 所在的同构类进行研究. 以下将对仿射 Weierstrass 方程进行化简，以便获得形式简单的同构类的代表元.

(1) 如果 K 的特征 $\mathrm{char}K \neq 2$ ，则可以消除 Y 项. 因为

$$\left(Y + \frac{1}{2}(a_1X + a_3)\right)^2 = \frac{a_1^2X^2 + 2a_1a_3X + a_3^2}{4} + X^3 + a_2X^2 + a_4X + a_6,$$

所以

$$\left(2\left(Y + \frac{1}{2}(a_1X + a_3)\right)\right)^2 = a_1^2X^2 + 2a_1a_3X + a_3^2 + 4X^3 + 4a_2X^2 + 4a_4X + 4a_6,$$

作变换

$$\begin{cases} X \longleftarrow X \\ Y \longleftarrow \dfrac{Y - (a_1X + a_3)}{2} \end{cases}$$

则得 $E' : Y^2 = 4X^3 + b_2X^2 + 2b_4X + b_6$ ，其中：

$$\begin{cases} b_2 = a_1^2 + 4a_2 \\ b_4 = 2a_4 + a_1a_3 \\ b_6 = a_3^2 + 4a_6 \end{cases}$$

(2) 如果 $\mathrm{char}K \neq 2,3$ ，则可以再消除 X^2 项. 作变换

$$\begin{cases} X \longleftarrow \dfrac{X - 3b_2}{36} \\ Y \longleftarrow \dfrac{Y}{108} \end{cases}$$

则得 $E'': Y^2 = X^3 - 27c_4X + 54c_6$, 显然, E'' 有奇异点当且仅当

$$f(X) = X^3 - 27c_4X + 54c_6$$

有重根，等价于 f 的判别式

$$\begin{aligned} d(f) &= 4 \times 27^3(c_4^3 - c_6^2) \\ &= (4 \times 27)^4 \times \Delta \quad (\text{见习题 } 1.7) \\ &= 0. \end{aligned}$$

因此，如果 $\mathrm{char}K \neq 2,3$ ，则 E'' ： $Y^2 = X^3 - 27c_4X + 54c_6$ 非奇异，当且仅当 $X^3 - 27c_4X + 54c_6$ 无重根，当且仅当 $c_4^3 - c_6^2 \neq 0$ ，即当且仅当 $\Delta \neq 0$.

(3) 如果 $\mathrm{char}K = 3$, 由 (1) 可知, 不妨设 E 为 $Y^2 = X^3 + a_2X^2 + a_4X + a_6$.

①如果 $a_2 = 0$ ，此时 $\Delta = -a_4^3$ 且 $c_4 = 0$ ，故若 $\Delta \neq 0$ 则 $j = 0$.

②如果 $a_2 \neq 0$ ，作变换

$$\begin{cases} X \longleftarrow X + \dfrac{a_4}{a_2}, \\ Y \longleftarrow Y \end{cases}$$

得 $E': Y^2 = X^3 + a_2'X^2 + a_6'$. 显然 $\Delta(E') = -a_2'^3a_6'$,$c_4' = a_2'^2$, 故若 $\Delta(E') \neq 0$ 则 $j(E') = -a_2'^3/a_6' \neq 0$.

(4) 如果 $\mathrm{char}K = 2$,

①若 $a_1 = 0$ ，作变换:

$$\begin{cases} X \longleftarrow X + a_2, \\ Y \longleftarrow Y \end{cases}$$

消去 X^2 项，得 $E': Y^2 + a_3'Y = X^3 + a_4'X + a_6'$ ， $\Delta(E') = a_3'^4$ 且 $c_4' = 0$ ，故若 $\Delta(E') \neq 0$ 则 $j(E') = 0$.

②若 $a_1 \neq 0$ ，作变换:

$$\begin{cases} X \longleftarrow a_1^2X + \dfrac{a_3}{a_1}, \\ Y \longleftarrow a_1^3Y + \dfrac{a_1^2a_4 + a_3^2}{a_1^3} \end{cases}$$

得到 $E': Y^2 + XY = X^3 + a_2'X^2 + a_6'$ ， $\Delta(E') = a_6'$ 且 $c_4' = 1$, 故若 $\Delta(E') \neq 0$ 有 $j(E') = 1/a_6'$.

以后将上述各情况下所获得的最终 Weierstrass 方程表示的曲线称为正规型，由上知任意一个 Weierstrass 方程都同构于某个正规型. 正规型的一些参数见表 1.1

表 1.1 正规型的一些参数

char$K$	正规型	j	Δ
$\neq 2,3$	$Y^2=X^3+a_4X+a_6$	$1728\dfrac{4a_4^3}{4a_4^3+27a_6^2}$	$-16(4a_4^3+27a_6^2)$
3	$Y^2=X^3+a_2X^2+a_6$	$-a_2^3/a_6\neq 0$	$-a_2^3a_6$
3	$Y^2=X^3+a_4X+a_6$	0	$-a_4^3$
2	$Y^2+XY=X^3+a_2X^2+a_6$	$1/a_6$	a_6
2	$Y^2+a_3Y=X^3+a_4X+a_6$	0	a_3^4

定理 1.3.4 Weierstrass 方程确定的曲线是仿射椭圆曲线，即是光滑的，当且仅当其判别式不为零.

证明 因为同构曲线间的判别式为非零常数倍的关系，且可允许变换不改变曲线的奇异性 (见习题 1.9)，所以只需对正规型证明结论成立.

(1) 当 char$K\neq 2,3$ 时，由前面的分析已知结论成立.

(2) 若 char$K=3$，

①设 $E:Y^2=X^3+a_2X^2+a_6$ 且 $a_2\neq 0$，因为 $\Delta=-a_2^3a_6$，故 $\Delta=0$ 当且仅当 $a_6=0$，即当且仅当 $(0,0)$ 是奇异点.

②设 $E:Y^2=X^3+a_4X+a_6$，此时 $\Delta=-a_4^3$，故 $\Delta=0$ 当且仅当 $a_4=0$，即当且仅当 $(0,\sqrt{a_6})$ 是奇异点.

(3) 若 char$K=2$，

①设 $E:Y^2+XY=X^3+a_2X^2+a_6$，此时 $\Delta=a_6$，故 $\Delta=0$ 当且仅当 $a_6=0$，即当且仅当 $(0,0)$ 是奇异点.

②设 $E:Y^2+a_3Y=X^3+a_4X+a_6$，此时

$$\Delta=a_3^4,$$
$$\frac{\partial E}{\partial X}=X^2+a_4,$$
$$\frac{\partial E}{\partial Y}=a_3.$$

因此，E 有奇异点当且仅当 $a_3=0$，当且仅当 $\Delta=0$，此时 $(\sqrt{a_4},\sqrt{a_6})$ 是其奇异点. 大家已经知道，令 E 是 K 上的仿射椭圆曲线，对任意 $P=(a,b)\in E$，

$O_P(E)$ 是离散赋值环，伴随着 $K(E)$ 上的一个赋值. 由定理 1.2.7 的证明过程可知在 P 的一致性参数 t_P 的具体取值如下.

(1) 若 $\mathrm{char}K \neq 2$，则 E 的等价形式为 $Y^2 = X^3 + a_2X^2 + a_4X + a_6$. 因为 $\dfrac{\partial E}{\partial Y} = 2Y$，所以 $\dfrac{\partial E}{\partial Y}|_P = 2b$, 故

$$t_P = \begin{cases} X - a, & 若b \neq 0, \\ Y, & 若b = 0. \end{cases}$$

(2) 若 $\mathrm{char}K = 2$，

①如果 $j \neq 0$， $Y^2 + XY = X^3 + a_2X^2 + a_6, a_6 \neq 0$. 因为 $\dfrac{\partial E}{\partial Y}|_{(a,b)} = a$, 故

$$t_P = \begin{cases} X + a, & 若a \neq 0, \\ Y + b, & 若a = 0. \end{cases}$$

②如果 $j = 0$，则 E 的等价形式为 $Y^2 + a_3Y = X^3 + a_4X + a_6, a_3 \neq 0$, 同上计算得 $t_P = X + a$. 故得 $K(E)$ 上的一个赋值

$$\mathrm{ord}_P : \begin{cases} K(E) \to Z \cup \{\infty\}, \\ \alpha = ut_P^d \to d, \\ 0 \to \infty, \end{cases}$$

其中， u 是 $O_P(E)$ 中的可逆元.

定义 1.3.5 对于 $r \in K(E)$和$P \in E, \mathrm{ord}_P(r)$ 称为 r 在 P 点的阶，或 r 在 P 的赋值. 若 $\mathrm{ord}_P(r) > 0$，则称 P 是 r 的零点；若 $\mathrm{ord}_P(r) < 0$，则称 P 是 r 的极点. 此时，零 (极) 点的重数为 $|\mathrm{ord}_P(r)|$.

1.4 椭 圆 曲 线

人们希望构造一个平面,满足任意两条曲线的交点个数等于它们的次数乘积. 考虑 $f(X,Y) \in K[X,Y]$ 和一条直线的交点，不妨设此直线过 $(0,0)$，即有参数方程

$$\begin{cases} X = \alpha t, \\ Y = \beta t, \end{cases} \tag{1.2}$$

将 $f(X,Y)$ 写成齐次式，即

$$f(X,Y) = f_n(X,Y) + f_{n-1}(X,Y) + \cdots + f_0,$$

其中，$f_i(X,Y)$ 是 i 次齐次式. 将式 (1.2) 代入上式得方程

$$f_n(\alpha,\beta)t^n + f_{n-1}(\alpha,\beta)t^{n-1} + \cdots + f_0(\alpha,\beta) = 0. \tag{1.3}$$

若 $f_n(\alpha,\beta) \neq 0$，则在代数闭域 K 中式 (1.3) 有 n 个解. 但若 $f_n(\alpha,\beta) = \cdots = f_{m+1}(\alpha,\beta) = 0, f_m(\alpha,\beta) \neq 0$，则式 (1.3) 有 m 个解. 在式 (1.3) 中做变化

$$t \leftarrow \frac{1}{s},$$

且两边乘以 s^n 得

$$f_n(\alpha,\beta) + \cdots + f_m(\alpha,\beta)s^{n-m} + \cdots + f_0(\alpha,\beta)s^n = 0.$$

可知，$s=0$ 为上式的 $n-m$ 重根，即 $t=\infty$ 为式 (1.3) 的 $n-m$ 重根. 添上 $t=\infty$ 可知 $f(X,Y)$ 和直线有 n 个根，因而必须将 $t=\infty$ 添加到直线上. 另外，在仿射平面内两条平行直线没有交点. 为了弥补这样的不足，试图在每条直线上添加一个“无穷远点”，且要满足相交直线各自的“无穷远点”不同，平行直线的各自的“无穷远点”相同. 显然直线的斜率能刻画“无穷远点”的这种特性. 故只需对过原点的直线添加“无穷远点”来扩展仿射平面即可获得所需结论.

定义 1.4.1 K 上的投射平面是 $K^3 \setminus \{(0,0,0)\}$ 在等价关系：

$$(x,y,z) \sim (x',y',z') \text{当且仅当存在} \lambda \in K^\times, \text{使得} (x',y',z') = (\lambda x, \lambda y, \lambda z),$$

下所得的等价类集合，记为 $P^2(K)$.$P^2(K)$ 中的元素称为投射点.

在不引起混淆的情况下,用 (x,y,z) 表示 (x,y,z) 所确定的投射点. $K[X,Y,Z]$ 中一个方程

$$f(X,Y,Z) = f_n(X,Y,Z) + \cdots + f_0(X,Y,Z)$$

要以投射点 $P=(x,y,z)$ 为零点，当且仅当对所有的 $t \in K^\times$ 有

$$f_n(x,y,z)t^n + \cdots + f_0(x,y,z) = 0$$

即 $f_i(x,y,z) = 0, 0 \leqslant i \leqslant n$，因而只需考虑齐次多项式的零点集即可. 将所有齐次多项式组成的集合记为 $K[X,Y,Z]_{\text{hom}}$. 齐次多项式一定是齐次不可约多项式的乘积.

定义 1.4.2 $K[X,Y,Z]$ 中的一个齐次不可约多项式 C 的零点集称为投射平面曲线.

设 U 是投射平面 P^2 的子集，其由所有 Z 坐标不为 0 的点组成，称为 P^2 的有限点，则 U 中的任意元素有唯一表示 $(x,y,1)$ ，即可由仿射点 (x,y) 表示. 故 A^2 和 U 之间存在 1-1 对应关系.

定义 1.4.3 映射

$$\begin{gathered}A^2 \to U\\(x,y) \mapsto (x,y)^* = (x,y,1),\\U \to A^2\\(x,y,z) \mapsto (x,y,z)_* = \left(\frac{x}{z},\frac{y}{z},1\right)_* = \left(\frac{x}{z},\frac{y}{z}\right)\end{gathered}$$

分别称为点相对于 Z 坐标的齐次化和齐次退化.

仿射平面 A^2 是投射平面的一个子集合，对多项式作适当的操作，可以使得仿射曲线上的仿射点恰好是相应的投射曲线在该子集合中的点.

以下将定义 $K[X,Y]$ 和 $K[X,Y,Z]_{\text{hom}}$ 间的齐次化和齐次退化，使得 $P \in A^2(K)$ 是 $f \in K[X,Y]$ 的零点当且仅当 P^* 是 f^* 的零点， $P \in U$ 是 $f \in K[X,Y,Z]_{\text{hom}}$ 的零点当且仅当 P_* 是 f_* 的零点. 齐次退化是容易定义的：因为 $f(x,y,1)=0$ 当且仅当 $f_*(x,y)=0$ ，故令 $f_* = f(X,Y,1)$ 即满足要求. 齐次化要求 $f\left(\frac{x}{z},\frac{y}{z}\right)=0$ 当且仅当 $f^*(x,y,z)=0$ ，因为 $f\left(\frac{X}{Z},\frac{Y}{Z}\right)$ 不是多项式，所以需要乘以 Z 的某个幂次，令 $f^* = Z^{\deg f} f\left(\frac{X}{Z},\frac{Y}{Z}\right)$ ，则 f^* 是多项式且满足要求. 自然还有相对于 X 或 Y 坐标的齐次化和齐次退化的映射. 投射平面可以看作是仿射平面上添加所有 Z 坐标为 0 的点构成的，这类点称为无穷远点.

定义 1.4.4 映射

$$\begin{gathered}K[X,Y] \to K[X,Y,Z]_{\text{hom}}\\f \mapsto f^* = Z^{\deg f} f\left(\frac{X}{Z},\frac{Y}{Z}\right),\\K[X,Y,Z]_{\text{hom}} \to K[X,Y]\\f \mapsto f_* = f(X,Y,1)\end{gathered}$$

分别称为相对于 Z 的齐次化和齐次退化.

命题 1.4.5 记 $f,g \in K[X,Y], F,G \in K[X,Y,Z]$ ，则有：

(1) $(fg)^* = f^*g^*$;

(2) $(FG)_* = F_* G_*$;

(3) $(f^*)_* = f$;

(4) $(F_*)^* = F$,若$Z \nmid F$.

推论 1.4.6 f 是仿射平面曲线当且仅当 f^* 是投射平面曲线. 此时, 称 f^* 是 f 的投射闭包. f^* 只比 f 多无穷远点.

定义 1.4.7 若 F 是投射平面曲线, 则 $R = \dfrac{K[X,Y,Z]}{(F)}$ 是整环, $L = R/\sim$ 是相应的分式域, 定义

$$K(F) = \{r = \frac{f}{g} : f, g \in R\text{且是齐次的}, \deg f = \deg g\},$$

显然 $K(F)$ 是域, 称为 F 的函数域. 称 $r \in K(F)$ 在 P 点正则, 若存在相同次数的齐次多项式 $f, g \in R$, 使得 $r = \dfrac{f}{g}$ 且 $g(P) \neq 0$. 定义

$$O_P(F) = \{r \in K(F) : r\text{在}P\text{点正则}\},$$

显然 $O_P(F)$ 是局部环, 称为 F 在 P 点的局部环.

由 f 与 f^* 的关系可以得到函数域间的同构映射:

$$\begin{aligned}
&K(f) \longrightarrow K(f^*), \\
&r = \frac{g}{h} \mapsto r^* = \frac{g^*}{h^*} Z^{\deg h - \deg g} = \frac{g\left(\dfrac{X}{Z}, \dfrac{Y}{Z}\right)}{h\left(\dfrac{X}{Z}, \dfrac{Y}{Z}\right)}, \\
&K(f^*) \longrightarrow K(f) \\
&\frac{G}{H} \mapsto \frac{G_*}{H_*} = \frac{G(X,Y,1)}{H(X,Y,1)},
\end{aligned}$$

所以

$$K(f) \cong K(f^*),$$
$$O_P(f) \cong O_{P^*}(f^*),$$

其中, $P = (a,b), P^* = (a,b,1)$, 显然对于 $r \in O_P(f)$, 有

$$r(P) = r^*(P^*).$$

注意：对于 $P=(a,b)$ ，取 $P^*=(a,1,b)$ 或 $(1,a,b)$ 有相类似的结论. 此时 f 对应的 f^* 分别为

$$f^* = Y^{\deg f} f\left(\frac{X}{Y}, \frac{Z}{Y}\right),$$
$$f^* = X^{\deg f} f\left(\frac{Y}{X}, \frac{Z}{X}\right).$$

例 1.6 求投射曲线 $F: Y=X$ 的赋值域，以及各点的一致性参数.

解 对 F 关于 Z 作齐次退化，得 $F_* = Y - X$ ，因为 $K(F) \cong K(F_*)$ ，

$$K[F_*] = K[X,Y]/(Y-X) = K[X],$$

所以 $K(F) \cong K(X)$. 对于 F 上的点 $(a,a,1), a \in K$, 对应于 F_* 上的点 (a,a) , 因为 (a,a) 的一致性参数为 $X-a$, 所以 $(a,a,1)$ 的一致性参数为 $(X-a)^* = X-aZ$. 对于 F 上的点 $(1,1,0)$ ，将 F 关于 X 作齐次退化，得 $F_* = Y-1$ ，则 $(1,1,0)$ 对应于 F_* 上的点 $(1,0)$. 同上可得

$$K[F_*] = K[Y,Z]/(Y-1) = K[Z],$$

$$K(F) \cong K(F_*) \cong K(Z),$$

因为 $(1,0)$ 的一致性参数为 Z ，所以 $(1,1,0)$ 的一致性参数为 $Z^* = Z/X$. 由 $K(Z) \cong K(F) \cong K(X)$ ，可得 F 关于 Z 作齐次退化后，$(1,1,0)$ 的一致性参数退化为 $1/X$.

定义 1.4.8 设 F 是投射平面曲线，P 是 F 上的点，若 P_* 是 F_* 的奇异点，则称 P 是 F 的奇异点，或 F 在 P 点奇异；否则，称 F 在 P 点光滑，定义 F 在 P 点的切线方程为 F_* 在 P_* 点切线方程的齐次化. 若 F 没有奇异点，则称 F 非奇异.

上述定义中的 P_* 与 F_* 是相对于 P 的某个取值非零的坐标所做的齐次退化，可以证明该定义是有意义的，即与坐标的选取无关 (见习题 1.11).

定理 1.4.9 投射平面曲线 F 在 P 点光滑，当且仅当

$$\left(\frac{\partial F}{\partial X}|_P, \frac{\partial F}{\partial Y}|_P, \frac{\partial F}{\partial Z}|_P\right) \neq (0,0,0).$$

证明 请读者自证 (见习题 1.12).

定理 1.4.10 设投射平面曲线 F 在 $P=(x_0,y_0,z_0)$ 点光滑，则 F 在 P 点的切线方程为

$$\frac{\partial F}{\partial X}|_{(x_0,y_0,z_0)}(X-x_0)+\frac{\partial F}{\partial Y}|_{(x_0,y_0,z_0)}(Y-y_0)+\frac{\partial F}{\partial Z}|_{(x_0,y_0,z_0)}(Z-z_0).$$

证明 不妨设 $z_0=1$，则 F_* 在 $P_*=(x_0,y_0)$ 点的切线方程为

$$l:\frac{\partial F_*}{\partial X}|_{(x_0,y_0)}(X-x_0)+\frac{\partial F_*}{\partial Y}|_{(x_0,y_0)}(Y-y_0),$$

令

$$\alpha=\frac{\partial F_*}{\partial X}|_{(x_0,y_0)},$$
$$\beta=\frac{\partial F_*}{\partial Y}|_{(x_0,y_0)},$$

则 F 在 P 点的切线为 $l^*:\alpha X+\beta Y+\gamma Z$, 其中 $\gamma=-\alpha x_0-\beta y_0$.

注意到

$$F(X,Y,Z)=Z^{\deg F}F_*\left(\frac{X}{Z},\frac{Y}{Z}\right),$$

显然

$$\frac{\partial F}{\partial X}|_{(x_0,y_0,1)}=\frac{\partial F_*}{\partial X}|_{(x_0,y_0)},$$
$$\frac{\partial F}{\partial Y}|_{(x_0,y_0,1)}=\frac{\partial F_*}{\partial Y}|_{(x_0,y_0)}.$$

考虑

$$\frac{\partial F}{\partial Z}=\deg FZ^{\deg F-1}F_*\left(\frac{X}{Z},\frac{Y}{Z}\right)+Z^{\deg F}\left(\frac{\partial F_*}{\partial X}\left(-\frac{X}{Z^2}\right)+\frac{\partial F_*}{\partial Y}\left(-\frac{Y}{Z^2}\right)\right),$$

则

$$\frac{\partial F}{\partial Z}|_{(x_0,y_0,1)}=-\alpha x_0-\beta y_0=\gamma.$$

令 l' 为

$$\frac{\partial F}{\partial X}|_{(x_0,y_0,z_0)}(X-x_0)+\frac{\partial F}{\partial Y}|_{(x_0,y_0,z_0)}(Y-y_0)+\frac{\partial F}{\partial Z}|_{(x_0,y_0,z_0)}(Z-z_0).$$

显然 $l'=l^*$.

若 $x_0=1$ 或 $y_0=1$，通过上述类似过程，可以得到和上式相同的切线方程. 请读者给出证明.

定义 1.4.11 仿射椭圆曲线的投射闭包称为椭圆曲线.

投射 Weierstrass 方程为

$$E: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3,$$

其判别式与 j 不变量的定义同仿射 Weierstrass 方程.

命题 1.4.12 投射 Weierstrass 方程不可约, 包含唯一的无穷远点 $O = (0,1,0)$, 且其决定的曲线奇异当且仅当 $\Delta = 0$.

证明 设 E 是投射 Weierstrass 方程. 因为

$$E_*: Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$$

不可约, 所以 E 不可约. 令 $P = (x, y, z) \in E$ 是无穷远点, 即 $z = 0$, 则 $x^3 = 0$, 所以

$$P = O,$$
$$E = E_* \cup \{(0,1,0)\}.$$

因为

$$\frac{\partial E}{\partial X}|_{(0,1,0)} = \frac{\partial E}{\partial Y}|_{(0,1,0)} = 0,$$
$$\frac{\partial E}{\partial Z}|_{(0,1,0)} = Y^2 = 1,$$

故 E 在 $(0,1,0)$ 点非奇异. 因为对于任意的 $P \in U \cap E$, 有

$$\frac{\partial E}{\partial X}|_P = \frac{\partial E_*}{\partial X}|_{P_*},$$
$$\frac{\partial E}{\partial Y}|_P = \frac{\partial E_*}{\partial Y}|_{P_*}.$$

而 E_* 奇异当且仅当 $\Delta = 0$, 所以 E 在 $U \cap E$ 上的某点奇异当且仅当 $\Delta = 0$, 由上知 E 奇异当且仅当 $\Delta = 0$.

显然, 椭圆曲线是非奇异投射 Weierstrass 方程定义的曲线. 投射 Weierstrass 方程决定的曲线

$$E: Y^2Z + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3;$$

$$E': Y^2Z + a_1'XYZ + a_3'YZ^2 = X^3 + a_2'X^2Z + a_4'XZ^2 + a_6'Z^3.$$

称为同构的，如果 E'_* 和 E_* 同构. 此时存在 $u \in K^{\times}, r,s,t \in K$ ，使得 E' 可由 E 通过如下变量替换

$$\begin{pmatrix} X \\ Y \\ Z \end{pmatrix} \mapsto \begin{pmatrix} u^2X + rZ \\ u^3Y + u^2sX + tZ \\ Z \end{pmatrix}$$

获得，如上形式的变换仍称为允许变换.

定理 1.4.13 对于椭圆曲线 E 和 $P \in E, O_P(E)$ 是离散赋值环. 若 $P = (a,b,1)$ ，则 E 在点 P 的一致性参数为 E_* 在点 (a,b) 的一致性参数 t_P 对应的 $K(E)$ 中的像 t_P^* ；若 $P = (0,1,0)$ ，则 E 在点 P 的一致性参数为 X/Y.

证明 对于 $P = (a,b,1)$ 已有结论 $O_P(E) \cong O_{P_*}(E_*)$ ，所以结论显然成立.

对于 $P = (0,1,0) = O$ ，已有结论 $O_O(E) \cong O_{O_*}(E_*)$ ，其中 $O_* = (0,0)$ ，此处的齐次退化是相对于 Y 的：

$$\begin{cases} E: & ZY^2 + a_1XYZ + a_3YZ^2 = X^3 + a_2X^2Z + a_4XZ^2 + a_6Z^3, \\ E_*: & z + a_1xz + a_3z^2 = x^3 + a_2x^2z + a_4xz^2 + a_6z^3, \end{cases}$$

因为

$$\frac{\partial E_*}{\partial z}|_{(0,0)} = 1,$$
$$\frac{\partial E_*}{\partial x}|_{(0,0)} = 0,$$

所以 E_* 在 $(0,0)$ 点的切线为 $\ell : z$ ， x 是 E_* 在点 O_* 的一致性参数，则 E 在 O 点的切线为 $\ell^* : Z/Y$ ， X/Y 是 E 在点 $P = (0,1,0)$ 的一致性参数. 结论证毕.

在 E_* 两边求 $\mathrm{ord}_{O_*}(x)$ ，因为

$$\mathrm{ord}_{O_*}(z) \geqslant 1, \qquad \mathrm{ord}_{O_*}(x) = 1,$$

所以左边为 $\mathrm{ord}_{O_*}(z)$ ，又因为

$$\mathrm{ord}_{O_*}(z) < \mathrm{ord}_{O_*}(a_2x^2z),$$
$$\mathrm{ord}_{O_*}(z) < \mathrm{ord}_{O_*}(a_4xz^2),$$
$$\mathrm{ord}_{O_*}(z) < \mathrm{ord}_{O_*}(a_6z^3),$$

而等式左右两边赋值应相等，故

$$\mathrm{ord}_{O_*}(z)=\mathrm{ord}_{O_*}(x^3)=3.$$
$$\mathrm{ord}_O\left(\frac{Z}{Y}\right)=3.$$
$$\mathrm{ord}_O\left(\frac{X}{Z}\right)=\mathrm{ord}_O\left(\frac{\frac{X}{Y}}{\frac{Z}{Y}}\right)=\mathrm{ord}_{O_*}\left(\frac{x}{z}\right)=\mathrm{ord}_{O_*}(x)-\mathrm{ord}_{O_*}(z)=-2.$$
$$\mathrm{ord}_O\left(\frac{Y}{Z}\right)=-\mathrm{ord}_{O_*}(z)=-3.$$

1.5 除子 (divisor)

将一个几何体用平面去切，得到的轨迹反映了几何体的局部性质. 当平面足够多时，就可能得到几何体的整体性质. 本节用曲线和椭圆曲线 E 的交点轨迹来刻画 E 的特性.

定义 1.5.1 (仿射) 直线 l 是指次数为 1 的多项式，即 $l=\alpha X+\beta Y+\gamma\in K[X,Y],\alpha,\beta$ 不全为 0.

定义 1.5.2 (交重数) 曲线 $f(X,Y)\in K[X,Y],P=(a,b)$ 为 f 上的一个点，设 l 为过 P 点的一条直线，其参数方程为

$$\begin{cases} X=a+\alpha t \\ Y=b+\beta t \end{cases} \qquad \alpha,\beta\in K.$$

如果 $f(a+\alpha t,b+\beta t)=ct^i+O(t^{i+1}),c\in K^\times$，则称 i 为 $f(X,Y)$ 和 l 在点 P 的交重数.

通过计算可知，椭圆曲线 E_* 上任意点 P 的一致性参数 t_P 所确定的直线与 E_* 在 P 的交重数为 1. 对于任意的 $r\in K[E_*]^\times$，存在 O_P 中的可逆元 u 和整数 d，使得 $r=ut_P^d$，则 r 与 E_* 在 P 的交重数为 d，即等于 $\mathrm{ord}_P(r)$. 所以形式和 $\sum\limits_{P\in E_*}\mathrm{ord}_P(r)<P>$ 恰好反映了 r 与 E_* 的交点. 由于 r 与 E_* 仅有有限个交点 (证明见定理 1.5.3)，所以 $\mathrm{ord}_P(r)$ 几乎对于所有的 P 为 0. 推而广之，有形式和

$$\sum_{P\in E} m_P<P>,\quad m_P\text{非负整数},\quad m_P\text{几乎处处为 } 0,$$

则这些元素的全体构成的集合对自然加法构成一个含幺、满足消去率的交换半群.此半群可以唯一地嵌入到以下的群中:

$$\mathrm{Div}(E)=\left\{D=\sum_{P\in E}m_P<P>:m_P\in\mathbb{Z},\text{几乎处处为}0\right\}$$

$\mathrm{Div}(E)$ 称为 E 的除子群, 其中的元素 D 称为 E 的除子 (divisor). $\sum\limits_{P\in E}m_P$ 称为 D 的次数, 记作 $\deg D$. 事实上, $\mathrm{Div}(E)$ 是 E 所生成的自由 Abel 群. 所有零次除子的全体构成 $\mathrm{Div}(E)$ 的一个子群, 记作 $\mathrm{Div}^0(E)$.

以下分析直线的齐次化 r 所确定的 E 的除子, 即 $\sum\limits_{P\in E}\mathrm{ord}_P(r)<P>$. 不妨设 r 相对于 Z 的齐次退化 r_* 为 $\alpha X+\beta Y+\gamma=0$, 其中 α,β,$\gamma\in K$.

(1) 如果 $\beta=0$, 则 $\alpha\neq 0$, 所以 r_* 可以表示为 $X=a$, 其中 $a\in K$.r_* 与 E_* 有两个有限交点

$$P=(a,b),$$
$$\overline{P}=(a,-b-a_1a-a_3),$$

其中 $b\in K$ 且满足

$$b^2+a_1ab+a_3b-(a^3+a_2a^2+a_4a+a_6)=0.$$

若 $P=\overline{P}$, 则 P 点的一致性参数为 $Y-b$, 所以 $\mathrm{ord}_P(X-a)=2$; 若 $P\neq\overline{P}$, 则 P 点的一致性参数为 $X-a$, 所以 $\mathrm{ord}_P(X-a)=1$. 对于无穷远点 O , 因为 $\mathrm{ord}_O(X)=-2$, 所以 $\mathrm{ord}_O(X-a)=-2$. 由上知 r 所确定的 E 的除子为

$$<P^*>+<\overline{P}^*>-2<O>.$$

(2) 如果 $\beta\neq 0$, 则 r_* 与 E_* 有三个有限交点, 记为 P_1,P_2,P_3 , 显然各点的重数均为 1. 对于无穷远点 O , 因为 $\mathrm{ord}_O(X)=-2,\mathrm{ord}_O(Y)=-3$, 所以 $\mathrm{ord}_O(r)=-3$. 由上知 r 所确定的 E 的除子为

$$<P_1^*>+<P_2^*>+<P_3^*>-3<O>.$$

显然, 直线 r 所确定的 E 的除子的次数均为 0.

定理 1.5.3 对于任意的 $r\in K[E]^\times$, 定义 $\mathrm{div}(r)=\sum\limits_{P\in E}\mathrm{ord}_P(r)<P>$, 则 $\mathrm{div}(r)$ 为 E 的除子, 且 $\deg(\mathrm{div}(r))=0$, 称 $\mathrm{div}(r)$ 为 r 所确定的 E 的除子.

证明 因为 r 没有有限极点，所以只需证 r 有有限个零点，且所有零点的重数之和等于 $|\mathrm{ord}_O(r)|$.

由于 $K(E_*)$ 是 $K(X)$ 的 Galois 扩张，设 $\mathrm{Gal}(K(E_*)/K(X)) = \{1, -\}$ ，则不妨设

$$N(r_*) = r_*\overline{r_*} = a(X-a_1)\cdots(X-a_d),$$

其中， $a, a_1, \cdots, a_d \in K, d \in \mathbb{N}, N(r_*)$ 表示 r_* 的范数，所以 $N(r_*)$ 有 d 个零点， $N(r_*)$ 与 E_* 有 $2d$ 个有限交点. 又因为如果 P 为 r_* 与 E_* 的交点，则 $\overline{P}$ 一定是 $\overline{r_*}$ 与 E_* 的交点，所以 r_* 与 E_* 共有 d 个有限交点，即 r_* 关于 E_* 有 d 个零点.

设 $r = u\left(\dfrac{X}{Z}\right) + v\left(\dfrac{X}{Z}\right)\dfrac{Y}{Z}$ ，因为 $\mathrm{ord}_O\left(\dfrac{X}{Z}\right) = -2, \mathrm{ord}_O\left(\dfrac{Y}{Z}\right) = -3$ ，所以

$$-\mathrm{ord}_O(r) = \max\{2\deg\ u, 2\deg\ v+3\},$$

计算得

$$N(r_*) = u^2 + \mathrm{Tr}(Y)uv + N(Y)v^2,$$

$$\mathrm{Tr}(Y) = -a_1X - a_3,$$

$$N(Y) = X^3 + a_2X^2 + a_4X + a_6,$$

所以

$$\deg\ N(r) = d = \max\{2\deg\ u, 2\deg\ v+3\}.$$

由上知 $\mathrm{div}(r)$ 是除子，且 $\deg(\mathrm{div}(r)) = 0$.

推论 1.5.4 对于任意的 $r \in K(E)^\times$ ，定义 $\mathrm{div}(r) = \sum\limits_{P\in E} \mathrm{ord}_P(r) < P >$ ，则 $\mathrm{div}(r)$ 为 E 的除子，且 $\deg(\mathrm{div}(r)) = 0$ ，称 $\mathrm{div}(r)$ 为 r 所确定的 E 的除子.

定义 1.5.5 有理函数 $r \in K(E)^\times$ 所确定的 E 的除子称为主除子；所有主除子的全体构成 $\mathrm{Div}(E)$ 的子群，称为主除子群，记作 $\mathrm{Prin}(E)$.$\mathrm{Div}(E)/\mathrm{Prin}(E)$ 记为 $\mathrm{Pic}(E)$ ，称为 Picard 群或除子类群；由推论 1.5.4 知道主除子的次数为 0 ，则 $\mathrm{Div}^0(E)/\mathrm{Prin}(E)$ 是有意义的，记其为 $\mathrm{Pic}^0(E)$ ，称为零次 Picard 群或零次除子类群.

定理 1.5.6 有理函数 $f \in K(E)$ 没有有限极点，当且仅当 $f_* \in K[E_*]$.

证明 由定理 1.5.3 的证明知， $K[E_*]$ 中的元素没有有限极点，且非常值多项式至少有两个零点.

设 $f_* = u + vY, u,v \in K(X)$，如果 f 没有有限极点，则 f_*，$\overline{f_*} = u + v\overline{Y}$ 也没有有限极点，从而 u,v 具有相同的有限极点或没有有限极点. 如果 u,v 没有有限极点，那么 $u,v \in K[X]$，即 $f_* \in K[E_*]$，结论得证；以下假设 u,v 有相同的有限极点. 因为 $f_*,\overline{f_*}$ 没有有限极点，所以 $f_* - \overline{f_*} = v(2Y + a_1X + a_3)$ 没有有限极点. 由于在允许变换下，极点的性质不发生改变，所以不妨设 E_* 的方程是正规型.

(1) 如果 $\mathrm{char}K \neq 2$，则 $a_1 = a_3 = 0$，$f_* - \overline{f_*} = 2vY$. 由于 $f_* - \overline{f_*}$ 没有有限极点，故 v 的有限极点一定是 Y 的零点，又因为 Y 的零点 P 形如 $(a,0)$，其中 a 满足

$$a^3 + a_2a^2 + a_4a + a_6 = 0,$$

所以如果 v 有有限极点，其一定为 P. 计算可得

$$\mathrm{ord}_P(Y) = 1,$$
$$\mathrm{ord}_P(X - a) = 2,$$

所以 $\mathrm{ord}_P(vY) \leqslant -1$，故如果 v 有有限极点，则 $f_* - \overline{f_*}$ 也有有限极点 (矛盾)，所以 v 没有有限极点.

(2) 如果 $\mathrm{char}K = 2, j = 0$，则 $a_1 = 0$，$f_* - \overline{f_*} = a_3v$，由于 $f_* - \overline{f_*}$ 没有有限极点，故 v 没有有限极点.

(3) 如果 $\mathrm{char}K = 2, j \neq 0$，则 $a_1 = 1, a_3 = 0$，$f_* - \overline{f_*} = vX$. 由于 $f_* - \overline{f_*}$ 没有有限极点，故 v 的有限极点一定是 X 的零点，又因为 X 的零点为 $P = (0, \sqrt{a_6})$，设

$$v = \frac{v_1}{X}, \qquad v_1 \in K[X],$$

如果 $v_1(0) = 0$，则 $v \in K[X]$，结论得证；如果 $v_1(0) \neq 0$，因为 u,v 有相同的有限极点，故

$$u = \frac{u_1}{X}, \qquad u_1 \in K[X], \qquad u_1(0) \neq 0,$$

则

$$f_* = \frac{u_1 + v_1Y}{X} = \frac{u_1(0) + v_1(0)Y}{X} + g(X,Y), \qquad g(X,Y) \in K[X,Y].$$

计算得

$$\mathrm{ord}_P(X) = 2,$$

$$\mathrm{ord}_P(Y-\sqrt{a_6})=1,$$
$$\mathrm{ord}_P\left(\frac{u_1(0)+v_1(0)Y}{X}\right)=-1,$$

而 $\mathrm{ord}_P(g(X,Y))\geqslant 0$ ，故 $\mathrm{ord}_P(f_*)=-1$ ，与 f_* 没有有限极点矛盾，所以 $v_1(0)=0$. 由以上证明知，f 没有有限极点当且仅当 $f_*\in K[E_*]$.

推论 1.5.7　设 D 是主除子，且存在 $f_1,f_2\in K(E_*)$ ，使得 $\mathrm{div}(f_1^*)=\mathrm{div}(f_2^*)=D$ ，那么 $\dfrac{f_1}{f_2}\in K^\times$.

定义 1.5.8　设 $D_1,D_2\in \mathrm{Div}(E)$ ，若存在 $f\in K(E_*)$ ，使得 $D_1=D_2+\mathrm{div}(f^*)$ ，则称 D_1 与 D_1 "线形等价"，记作 $D_1\sim D_2$.

通过计算直线与椭圆曲线 E 的交点，得以下结论：

(1) $\mathrm{div}(X-a)=<P>+<\overline{P}>-2<O>$;

(2) $\mathrm{div}(Y-(mX+\lambda))=<P>+<Q>+<R>-3<O>$.

定理 1.5.9　对于一条直线 l 和椭圆曲线 E_* 上的交点 $P=(a,b)$ ，$\mathrm{ord}_P(l)\geqslant 2$ ，当且仅当 l 是点 P 相对于 E_* 的切线.

证明　P 相对于 E_* 的切线 t 为

$$\frac{\partial E_*}{\partial X}|_P(X-a)+\frac{\partial E_*}{\partial Y}|_P(Y-b),$$

因为 E_* 在函数域 $K(E_*)$ 中为 0 ，根据 E_* 在 P 点的泰勒展开式，可知 t 还可以表示为

$$-\frac{\partial E_*}{\partial X^2}|_P(X-a)^2-\frac{\partial E_*}{\partial X\partial Y}|_P(X-a)(Y-b)-\frac{\partial E_*}{\partial Y^2}|_P(Y-b)^2-\cdots,$$

由于 $\mathrm{ord}_P(X-a)\geqslant 1,\mathrm{ord}_P(Y-b)\geqslant 1$ ，所以 $\mathrm{ord}_P(t)\geqslant 2$.

如果 $\mathrm{ord}_P(l)\geqslant 2$ ，欲证 l 是切线. 不妨设 l 为 $\alpha(X-a)+\beta(Y-b),\alpha,\beta$ 不同时为 0. 若 $P=\overline{P}$ ，即 $\dfrac{\partial E_*}{\partial Y}|_P=0$ ，所以 $Y-b$ 是点 P 的一致性参数，$X-a$ 为切线，又因为 $\mathrm{ord}_P(l)\geqslant 2$ ，故 $\beta=0$ ，l 为切线；若 $P\neq\overline{P}$ ，则 $X-a$ 为点 P 的一致性参数，$\beta=0$ 意味着 $\mathrm{ord}_P(l)=1$ ，与已知矛盾，所以 $\beta\neq 0$ ，不妨设 $\beta=1$. 由 $\mathrm{ord}_P(l)\geqslant 2$ 知

$$F(X)=E_*(X,-\alpha(X-a)+b)=0$$

有重根 a ，即

$$\frac{\partial F}{\partial X}|_{X=a}=\frac{\partial E_*}{\partial X}+\frac{\partial E_*}{\partial Y}(-\alpha)|_P,$$

得

$$\alpha = \frac{\frac{\partial E_*}{\partial X}|_P}{\frac{\partial E_*}{\partial Y}|_P},$$

所以 l 为切线. 证毕.

定理 1.5.10 任意给定 $P,Q \in E$ 不同时为 O，则存在一条直线 ℓ 和一个点 R，使得: $\mathrm{div}(l^*) =< P > + < Q > + < R > -3 < O >$.

证明 以下分情况讨论:

(1) 若 P,Q 中有一个为 O，不妨设 $P = (a,b,1), a,b \in K, Q = O$，那么有

$$\mathrm{div}(X-a) = P + \bar{P} - 2 < O >,$$

所以 l 为 $X-a$, R 为 $\bar{P}$.

(2) 若 $P \neq O, Q \neq O, P \neq Q$，设 $P = (a_1, b_1, 1), Q = (a_2, b_2, 1), a_1, a_2, b_1, b_2 \in K$.

①若 $P = \overline{Q}$, 显然 l 为 $X-a$， R 为 O.

②若 $P \neq \overline{Q}$，则必有 $a_1 \neq a_2$，作过 P,Q 的直线 $Y = \lambda X + u$，可知

$$\lambda = \frac{b_2 - b_1}{a_2 - a_1},$$
$$u = b_1 - \lambda a_1,$$

则 l 即为 $Y = \lambda X + u$， R 为该直线与 E 相交的第三点.

(3) $P \neq O, Q \neq O, P = Q$，令 l 为点 P 相对于 E 的切线, 则 $\mathrm{ord}_P(l) \geqslant 2$，所以 l 满足要求， R 为 l 与 E 相交的第三点.

定理 1.5.11 令 $D \in \mathrm{Div}(E)$，那么存在唯一 $P \in E$，使得

$$D \sim < P > + (\deg D - 1) < O > .$$

证明 不妨设

$$D = \sum_{Q \in E \setminus \{O\}} m_Q < Q > + m < O >,$$
$$\mathrm{supp} D = \{Q \in E : m_Q \neq 0\}.$$

若 $m_Q < 0$，设 $Q = (a,b,1)$，因为

$$\mathrm{div}((X-a)^*) =< Q > + < \overline{Q} > -2 < O >,$$

所以 $-<Q>\sim<\overline{Q}>-2<O>$，可得

$$m_Q<Q>\sim -m_Q<\overline{Q}>+2m_Q<O>.$$

故在等价意义下，不妨设 $m_Q \geqslant 0$.

若 $m_Q \geqslant m_{\overline{Q}}$，因为 $<Q>+<\overline{Q}>\sim 2<O>$，所以

$$m_Q<Q>+m_{\overline{Q}}<\overline{Q}>=(m_Q-m_{\overline{Q}})<Q>+m_{\overline{Q}}(<Q>+<\overline{Q}>)$$

线性等价于 $(m_Q-m_{\overline{Q}})<Q>+2m_{\overline{Q}}<O>$. 故在等价意义下，可以要求 $Q,\overline{Q}$ 不同时属于 $\mathrm{supp}D$.

又因为存在 R，使得 $2<Q>\sim<\overline{R}>+<O>$, 所以可以要求如果 $Q\in\mathrm{supp}D$, 则 $m_Q=1$.

通过以上可知 D 必线性等价于

$$\sum_{i=1}^{t}<Q_i>+n<O>,\qquad n+t=\deg D,$$

且 Q_i 两两不共轭. 则因为存在 R 使得

$$<Q_1>+<Q_2>\sim<\overline{R}>+<O>,$$

所以

$$D\sim<\overline{R}>+\sum_{i=3}^{t}<Q_i>+(n+1)<O>,$$

递推下去，可得存在 P，使得 $D\sim<P>+(\deg D-1)<O>$.

若还存在 Q，使得 $D\sim<Q>+(\deg D-1)<O>$，则 $<P>-<Q>$ 为主除子，因为存在 R 使得

$$<P>-<Q>\sim<P>+<\overline{Q}>-2<O>\sim<R>-<O>,$$

设 $\mathrm{div}(f^*)=<R>-<O>$，由于 f^* 没有有限极点，所以 f 为多项式，又因为非常值多项式至少有两个有限零点，故 f 为常值，则 $R=O,P=Q$. 证毕.

推论 1.5.12 令 $D\in\mathrm{Div}^0(E)$，那么存在唯一 $P\in E$，使得 $D\sim<P>-<O>$.

推论 1.5.13 $\mathrm{Pic}^0(E)$ 与 E 间存在双射:

$$\begin{aligned} &\mathrm{Pic}^0(E) \to E \\ \phi : &\overline{<P>-<O>} \mapsto P \\ \psi : &\overline{<P>-<O>} \leftarrow\!\!\shortmid P \end{aligned}$$

因为 $\mathrm{Pic}^0(E)$ 具有群结构, 所以可以在 E 上定义群结构: 对于 $P,Q \in E$, 定义

$$P+Q=\phi(\psi(P)+\psi(Q)).$$

显然,

$$\begin{aligned} \phi(0) &= O, \\ nP &= \sum_{i=1}^{n} P = \phi(\overline{n<P>-n<O>}), \\ P+O &= \phi(\overline{<P>-<O>}+0) = P, \\ P+\overline{P} &= \phi(\overline{<P>-<O>}+\overline{<\overline{P}>-<O>}) = \phi(0) = O. \end{aligned}$$

定理 1.5.14 $D=\sum_{P\in E} n_P <P> \in \mathrm{Div}^0(E)$ 是主除子, 当且仅当 $\sum_{P\in E} n_P P = 0$.

证明 D 可以表示为 $\sum_{P\in E\backslash\{O\}} n_P(<P>-<O>)$, 所以 $\phi(D) = \sum_{P\in E\backslash\{O\}} n_P P$. D 是主除子, 当且仅当 $D\sim 0$, 当且仅当 $\phi(D)=O$, 即 $\sum_{P\in E} n_P P = O$. 证毕.

定理 1.5.15 设椭圆曲线 E,E' 有同构映射 $\phi : E \to E'$, 则作为群有 $E \cong E'$.

证明 只需证 $\mathrm{Pic}^0(E) \cong \mathrm{Pic}^0(E')$. 设 $\psi : K(E) \to K(E')$ 是相应的允许变换. 由 ϕ 可诱导如下映射:

$$\begin{aligned} &\mathrm{Div}^0(E) \to \mathrm{Pic}^0(E') \\ D = \sum_{P\in E\backslash\{O\}} n_P(<P>-<O>) &\mapsto \overline{\sum_{P\in E\backslash\{O\}} n_P(<\phi(P)>-<O>)} \end{aligned}$$

仍记为 ϕ. 若 $\phi(D)=0$, 即存在 $f' \in K(E')$, 使得

$$\mathrm{div}(f') = \sum_{P\in E\backslash\{O\}} n_P(<\phi(P)>-<O>),$$

其中, $n_P = \mathrm{ord}_{\phi(P)}(f')$. 因为 $\psi^{-1}(f') \in K(E)$, $\mathrm{ord}_{\phi(P)}(f') = \mathrm{ord}_P(\psi^{-1}(f'))$, 所以 $D = \mathrm{div}(\psi^{-1}(f'))$, 即 $\mathrm{Prin}(E) \supseteq \mathrm{Ker}(\phi)$. 对于任意的 $f \in K(E)$, 令 $D = \mathrm{div}(f)$, 因为 $\mathrm{ord}_P(f) = \mathrm{ord}_{\phi(P)}(\psi(f))$, 所以 $\phi(D) = \mathrm{div}(\psi(f))$, 因为 $\psi(f) \in K(E')$, 所以 $\phi(D) = 0$, $\mathrm{Prin}(E) \subseteq \mathrm{Ker}(\phi)$. 由于 E 与 E' 间的点一一对应, 所以 ϕ 是满射. 同态显然. 故 $\mathrm{Pic}^0(E) \cong \mathrm{Pic}^0(E')$, 即 $(E,+) \cong (E',+)$. 证毕.

加法公式: 设 $P = (x_1, y_1, 1), Q = (x_2, y_2, 1)$

①若 $Q = \bar{P}$, 则 $P + Q = O$.

②若 $Q \neq \bar{P}$, 则过 P,Q 的直线为 $\ell : Y - (\lambda X + u)$, 其中

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & \text{若 } P \neq Q \\ \dfrac{3x_1^2 + 2a_2x_1 + a_4 - a_1y_1}{2y_1 + a_1x_1 + a_3}, & \text{若 } P = Q \end{cases}$$

设 $R = (x_3, y_3, 1)$, 满足 $R + P + Q = O$, 则 $-(X - x_1)(X - x_2)(X - x_3) = E_*(X, \lambda X + u)$, 比较两边 X^2 的系数得 $x_1 + x_2 + x_3 = \lambda^2 + a_1\lambda - a_2$, 因此,

$$\begin{cases} x_3 = \lambda^2 + a_1\lambda - a_2 - x_1 - x_2 \\ y_3 = \lambda x_3 + u \end{cases}$$

故 $P + Q = \bar{R} = (x_3, -y_3 - a_1x_3 - a_3) = (x_3, -(\lambda + a_1)x_3 - a_3 - u)$

注意:

(1) 对三种正规型有更简单的公式.

(2) $(x_1, y_1, z_1) + (x_2, y_2, z_2) = (x_3, y_3, z_3)$ 用投射坐标表示, 可以不用除法.

推论 1.5.16 若 E 定义在 $k \subseteq K$ 上, 定义 $E(k) = \{(x, y) \in k^2 : E(x, y) = 0\} \cup \{O\}$, 则 $E(k)$ 是 E 的子群.

例 1.7 给定 $\mathbb{F}_4 = \{0, 1, \alpha, \alpha+1\}, \alpha^2 = \alpha+1$, $E : Y^2 + Y = X^3 + X + 1$, 则

$$E(\mathbb{F}_4) = \{P_1 = (0, \alpha), P_2 = (0, \alpha + 1), P_3 = (1, \alpha), P_4 = (1, \alpha + 1)\} \cup \{O\},$$

可以验证

$$-P_1 = (0, \alpha + 1) = P_2,$$

$$2P_1 = (1, \alpha) = P_3,$$

$$-2P_1 = (1, \alpha + 1) = P_4,$$

$$3P_1 = O.$$

习 题 一

1.1 毕达哥拉斯三元数组 (a,b,c) 满足 $a^2+b^2=c^2$ ， a 是奇数， b 是偶数. 则存在 $(m,n)\in\mathbb{Z}^2$ 使得

$$(a,b,c)=(m^2-n^2,2mn,m^2+n^2).$$

1.2 $C_1,C_2\in K[X,Y]$ 是不可约多项式，则 $C_1\neq C_2$ 当且仅当 $C_1(K)\neq C_2(K)$.

1.3 若 X 在域 K 上超越，且 F 是 $K(X)$ 的有限代数扩张，则称 F 是 K 的单变量函数域. F 的子域

$$\tilde{K}=\{z\in F: z\text{是}K\text{的代数元}\}$$

称为 F/K 的常值域. 证明定义 1.2.5 中的 $K(C)$ 是以 K 为常值域的单变量函数域.

1.4 令 $R=K[X,Y]$ ，定义 R 的 Krull 维数为 R 的素理想链的最大长度，记为 $\dim R$ ，则 $\dim R=2$ 且每个极大理想都有形式 $(X-a,Y-b)$ ，其中 $a,b\in K$.

1.5 R 是交换环，则下述条件等价：

① R 的每个理想是主理想；

② R 的每个素理想是主理想.

1.6 令 $f\in K[X,Y]$ ，则 f 在 $K[X,Y]$ 中不可约当且仅当 f 在 $K(X)[Y]$ 中不可约.

1.7 证明 $1728\Delta=c_4^3-c_6^2$.

1.8 设 Weierstrass 方程 E 的判别式 $\Delta=0$ ，则 E 有且只有一个奇异点.

1.9 Weierstrass 方程所决定的曲线是光滑的，当且仅当允许变换后方程所决定的曲线是光滑的.

1.10 仿射椭圆曲线 E 上的两个不同点 $P=(a,b),P'=(a',b')$ 的局部环 $O_P(E)$ 和 $O_{P'}(E)$ 互不相同.

1.11 设 $P=(a,b,c)$ 是投射平面曲线 F 的奇异点，则相对于 X,Y 或 Z 作齐次退化，均有 P_* 是 F_* 的奇异点，其中 $a\neq 0,b\neq 0,c\neq 0$.

1.12 投射平面曲线 F 在 P 点光滑，当且仅当

$$\left(\frac{\partial F}{\partial X}|_P,\frac{\partial F}{\partial Y}|_P,\frac{\partial F}{\partial Z}|_P\right)\neq(0,0,0).$$

第 2 章　有限域上的椭圆曲线

上一章已证明任意域上的椭圆曲线点构成加法群，且椭圆曲线点的加法公式完全由域运算组成. 为了便于设计椭圆曲线公钥密码体制，既要选择可计算的域，使得其上的椭圆曲线点的加法能有效实现，又要使构成的加法群是一个有限群. 显然，有限域满足这样的要求.

令 $k = \mathbb{F}_q$ 是 q 元有限域，其特征为 p，记其代数闭包为 $K = \overline{k}$.E 为 k 上的一条椭圆曲线，即其系数 a_1, a_3, a_2, a_4, a_6 均属于 k，则称 k 是 E 的基域. 同前，仍用 E 表示该曲线在 K 上的所有点构成的群，$E(k)$ 表示 k 有理点构成的群，即在 k 上取值的 E 点构成的群. 因为 k 是有限阶的，所以 $E(k)$ 是有限阿贝尔群. 本章主要任务是给出 $E(k)$ 的阶估计和 $E(k)$ 的群结构.

2.1　有理映射和同种

令 E,E' 均是定义在 K 上的椭圆曲线, 其系数分别用 $\{a_i\}_{1\leqslant i\leqslant 6}$ 和 $\{a'_i\}_{1\leqslant i\leqslant 6}$ 表示. 由前可知，除了有限个极点外，有理函数可以看作是椭圆曲线 E 到其基域 K 的映射. 本节定义 E 到椭圆曲线 E' 的映射. 对于有理函数三元组 $\alpha = (\alpha_1,\alpha_2,\alpha_3) \in \mathbb{P}^3(K(E))$, 任意 $P \in E$，可不妨设 $\alpha_1, \alpha_2, \alpha_3$ 均在 P 点正则. 此时 $\alpha(P) = (\alpha_1(P), \alpha_2(P), \alpha_3(P))$. 若 α 是 E 到 E' 的映射，则 $\alpha(P)$ 是 E' 上的点，即

$$(E' \circ \alpha)(P) = E'(\alpha(P)) = 0, \qquad \forall P \in E.$$

故有以下定义:

定义 2.1.1　*E 到 E' 的有理映射是指椭圆曲线 $E'(K(E))$ 上的点. 将 E' $(K(E))$ 中的无穷远点记作 $[0]$.*

因为 $E'(K(E))$ 中 Z 坐标为 0 的点只有无穷远点，记为有理映射 $[0]$，而 $[0]$ 作用于 E 上的点所得像的 Z 坐标为 0，E' 中 Z 坐标为 0 的点只有 O，所以 $[0]$ 将 E 上的所有点均映射到 O；对于 Z 坐标不为 0 的有理映射均可以表示为 $\alpha = (\alpha_1, \alpha_2, 1)$，故以下可以将非 $[0]$ 有理映射简记为 $\alpha = (\alpha_1, \alpha_2)$. 对于 $\alpha = (\alpha_1, \alpha_2)$，任取 $P \in E$，有

$$\alpha_2^2 + a'_1\alpha_1\alpha_2 + a'_3\alpha_2 = \alpha_1^3 + a'_2\alpha_1^2 + a'_4\alpha_1 + a'_6.$$

若 $\mathrm{ord}_P\alpha_1 < 0, \mathrm{ord}_P\alpha_2 \geqslant 0$ ，则等式左边在 P 的赋值不小于 $\mathrm{ord}_P\alpha_1$ ，而等式右边在 P 的赋值等于 $3\mathrm{ord}_P\alpha_1$ ，显然 $3\mathrm{ord}_P\alpha_1 < \mathrm{ord}_P\alpha_1$ ，产生矛盾；同理可知 $\mathrm{ord}_P\alpha_1 \geqslant 0, \mathrm{ord}_P\alpha_2 < 0$ 也不会同时成立；所以 α_1,α_2 在 P 点或者均正则或者均不正则. 若 α_1,α_2 正则，则 $\alpha^*(P) = (\alpha_1(P), \alpha_2(P), 1)$ ， $\alpha(P) = (\alpha_1(P), \alpha_2(P)) = \alpha^*(P)_*$. 若 α_1,α_2 不正则，不妨设 $u \in K(E)$ 是 P 的一致性参数， $d = \min\{\mathrm{ord}_P(\alpha_1), \mathrm{ord}_P(\alpha_2)\} < 0$ ，则 $\alpha^* = (u^{-d}\alpha_1, u^{-d}\alpha_2, u^{-d})$ ，因为 $u^{-d}(P) = 0$ ，所以 $\alpha^*(P) = O$ ，补充定义 $\alpha(P) = O$. 由此可得

$$\alpha(P) = \begin{cases} (\alpha_1(P), \alpha_2(P)), & \text{若}\alpha_1, \alpha_2\text{在}P\text{点均正则;} \\ O, & \text{若}\alpha_1, \alpha_2\text{在}P\text{点均不正则.} \end{cases}$$

因为在椭圆曲线的加法法则下所有的有理映射构成一个群. 由此带来一个疑问，对于 E 上的点 P ，两个有理映射的和在其上的像与两个有理映射在其上的像的和相等吗？

定理 2.1.2 设 α,β 是 E 到 E' 上的两个有理映射，则

$$(\alpha + \beta)(P) = \alpha(P) + \beta(P), \qquad \forall P \in E.$$

证明 仅给出 $p \neq 2,3$,

$$E : Y^2 = X^3 + a_4X + a_6,$$

$$E' : Y^2 = X^3 + a_4'X + a_6'$$

下的证明， $p = 2,3$ 的情况请读者作为练习题 (见习题 2.1). 给定椭圆曲线 E 上的一个点，记为 P.

(1) 若 $\alpha = [0]$ 或 $\beta = [0]$ ，则结论显然成立.

(2) 否则令 $\alpha = (\alpha_1, \alpha_2), \beta = (\beta_1, \beta_2)$.

①若 $\alpha = -\beta$ ，则 $\alpha_1 = \beta_1, \alpha_2 = -\beta_2, \alpha + \beta = [0]$. 如果 $\alpha_1 = \beta_1$ 在 P 不正则，则 $\alpha(P) + \beta(P) = O + O = O = [0](P) = (\alpha + \beta)(P)$ ；否则，$\alpha_1(P) = \beta_1(P), \alpha_2(P) = -\beta_2(P)$, 即 $\alpha(P) = -\beta(P)$, 所以 $\alpha(P)+\beta(P) = O$.

②若 $\alpha + \beta \neq [0]$ ，令 $\alpha + \beta = \gamma = (\gamma_1, \gamma_2)$. 如果 $\alpha \neq \beta$ ，则

$$\gamma_1 = -\alpha_1 - \beta_1 + \lambda^2,$$

$$\gamma_2 = \lambda(\alpha_1 - \gamma_1) - \beta_1,$$

$$\lambda = \frac{\beta_2 - \alpha_2}{\beta_1 - \alpha_1}.$$

a. 如果 $\alpha(P)$ 和 $\beta(P)$ 是互不相同的有限点，且 $\alpha(P) \neq -\beta(P)$，则将 P 代入以上各式，即得 $\alpha(P) + \beta(P)$，所以 $\gamma(P) = \alpha(P) + \beta(P)$.

b. 如果 $\alpha(P)$ 和 $\beta(P)$ 是互不相同的有限点,但 $\alpha(P) = -\beta(P)$,则 $\alpha_1(P) = \beta_1(P)$, $\alpha_2(P) \neq \beta_2(P)$，所以 P 是 λ 的极点，进一步， P 是 γ_1 的极点，故 $\gamma(P) = O = \alpha(P) + \beta(P)$.

c. 如果 $\alpha(P) = \beta(P)$ 是有限点，且不是 2 阶点，即 $\alpha_1(P) = \beta_1(P)$ 记作 x， $\alpha_2(P) = \beta_2(P)$ 记作 y, 且 $2y \neq 0$. 因为 $(\alpha + \beta)(P)$ 和 $\alpha(P) + \beta(P)$ 的公式中唯一的差别是 λ 的定义不同，若记

$$\lambda' = \frac{3\alpha_1^2 + a_4'}{2\alpha_2},$$

则 $\alpha(P)$,$\beta(P)$ 确定的直线的斜率为 $\lambda'(P)$. 只需证明 $\lambda(P) = \lambda'(P)$，即可得

$$\begin{aligned}
\gamma(P) &= \alpha(P) + \beta(P) \\
\lambda &= \frac{\beta_2 - \alpha_2}{\beta_1 - \alpha_1} \\
&= \frac{\beta_2 - \alpha_2}{\beta_1 - \alpha_1} \cdot \frac{\beta_2 + \alpha_2}{\beta_2 + \alpha_2} \\
&= \frac{\beta_1^3 + a_4'\beta_1 - \alpha_1^3 - a_4'\alpha_1}{(\beta_1 - \alpha_1)(\beta_2 + \alpha_2)} \\
&= \frac{\beta_1^2 + \beta_1\alpha_1 + \alpha_1^2 + a_4'}{\beta_2 + \alpha_2},
\end{aligned}$$

将 $\alpha(P) = \beta(P) = (x, y)$ 代入得

$$\lambda(P) = \frac{3x^2 + a_4'}{2y} = \lambda'(P).$$

d. 如果 $\alpha(P) = \beta(P)$ 是有限点，且阶为 2. 由上可知

$$\lambda = \frac{\beta_1^2 + \beta_1\alpha_1 + \alpha_1^2 + a_4'}{\beta_2 + \alpha_2},$$

所以 λ 在 P 的取值的分母为 $\dfrac{\partial E'}{\partial Y}(\alpha(P))$，分子为 $\dfrac{\partial E'}{\partial X}(\alpha(P))$，由于 $\alpha(P)$ 是 2 阶元，所以 $\dfrac{\partial E'}{\partial Y}(\alpha(P)) = 0, \dfrac{\partial E'}{\partial X}(\alpha(P)) \neq 0$, 故 P 是 λ 的极点，也是 γ 的极点，则 $\gamma(P) = O = 2\alpha(P)$.

e. 如果 $\alpha(P)$,$\beta(P)$ 中有一个为无穷远点，不妨设 $\alpha(P)=O$ ，则

$$\alpha_1 = u^{d_1}\alpha_1',$$
$$\alpha_2 = u^{d_2}\alpha_2',$$

其中， u 是点 P 的一致性参数， $d_1,d_2<0, P$ 既不是 α_1',α_2' 的极点，也不是它们的零点．下面证明 $\gamma(P)$ 为有限点．因为 $E(\alpha_1,\alpha_2)=0$ ，所以 $2d_2=3d_1$ ，将 λ 代入 γ_1 得

$$\gamma_1 = \frac{(\alpha_1\beta_1+a_4')(\alpha_1+\beta_1)-2\alpha_2\beta_2+2a_6'}{(\alpha_1-\beta_1)^2}.$$

由 $\beta(P)$ 是有限点知 $\mathrm{ord}_P(\beta_1),\mathrm{ord}_P(\beta_2)\geqslant 0$ ，所以

$$\begin{aligned}\mathrm{ord}_P(\gamma_1)&\geqslant \min\{2d_1,d_2\}-2d_1=\min\{0,d_2-2d_1\}\\&=\min\left\{0,-\frac{1}{2}d_1\right\}=0.\end{aligned}$$

即得 $\gamma(P)$ 为有限点，由于 $\alpha=\gamma-\beta$ ， $\gamma(P)$,$\beta(P)$ 均为有限，已证 $\alpha(P)=\gamma(P)-\beta(P)$ ，所以 $\gamma(P)=\alpha(P)+\beta(P)$.

f. 如果 $\alpha(P)=\beta(P)=O$ ，若 $\gamma(P)\neq O$ ，因为 $\alpha=\gamma-\beta$ ，由上可知

$$O=\alpha(P)=\gamma(P)-\beta(P)=\gamma(P),$$

矛盾，所以 $\gamma(P)=O$.

③如果 $\alpha=\beta\neq-\beta$ ，则 $\lambda=\dfrac{3\alpha_1^2+a_4'}{2\alpha_2}$.

a. 如果 $\alpha(P)\neq O$ ，则将 P 代入 γ_1,γ_2, 即得 $\gamma(P)=2\alpha(P)$.

b. 如果 $\alpha(P)=O$ ，若 $\gamma(P)\neq O$ ，则 $\alpha=\gamma-\alpha$ ，由前可知

$$O=\alpha(P)=\gamma(P)-\alpha(P)=\gamma(P),$$

矛盾，所以 $\gamma(P)=O$.

例 2.1 恒等映射 $id=(X,Y)$ 和常值映射 $c_Q=(x,y)$, 显然是 E 到自身的有理映射，其中 $Q=(x,y)\in E$. 定义 Q 平移映射

$$\begin{aligned}\tau_Q: E&\to E\\ P&\mapsto P+Q.\end{aligned}$$

则 $\tau_Q = id + c_Q$，所以 τ_Q 也是 E 到自身的有理映射.

命题 2.1.3 有理映射要么是常值映射，要么是满射.

证明 首先证明有理函数作用于 E 的像集要么仅为 K 中的一个元素，要么为 K. 假设 r 是非常值有理函数，则 r 一定有零点. 对于任意的 $x \in K$，$r - x$ 也一定有零点，不妨记为 P，则 $(r-x)(P) = r(P) - x = 0$，所以 r 对应的像集为 K.

结论对于 [0] 显然成立. 设有理映射

$$\alpha = (\alpha_1, \alpha_2) : E \to E'.$$

如果 α_1 是常值有理函数，则 α_2 作用于椭圆曲线 E 上的点所得的像一定为 $E'(\alpha_1, Y) \in K[Y]$ 在 K 中的根，因为根的个数有限，所以 α_2 不是满射，故 α_2 是常值有理函数，即 α 是常值映射；如果 α_1 不是常值有理函数，则 α_1 一定有一个零点，进一步，α_1 也有一个极点记为 P，所以 $\alpha(P) = O$. 将该结论应用于有理映射 $\tau_{-Q} \circ \alpha$，可知存在点 $P \in E$，使得 $\tau_{-Q} \circ \alpha(P) = \alpha(P) - Q = O$，其中 Q 为 E' 中的任意点，所以 α 是满射.

定义 2.1.4 具有群同态性质的有理映射称为 E 到 E' 的同种 (isogeny).E,E' 称为同种的 (isogenous)，如果存在从 E 到 E' 的同种映射. 如果该同种映射是定义在 k 上的，则称 E,E' 是 k 同种的. E 到 E 的同种称为 E 的自同态 (endomorphism)，E 的所有自同态组成的集合记为 $\mathrm{End}(E)$.

命题 2.1.5 $\mathrm{End}(E)$ 是环，其中自同态的乘法运算定义为自同态的复合运算.

证明 只需证明满足分配率. 设 α,β,γ 是自同态，则对于任意的 $P \in E$ 有

$$\begin{aligned}(\alpha \circ (\beta + \gamma))(P) &= \alpha((\beta + \gamma)(P)) \\ &= \alpha(\beta(P) + \gamma(P)) \\ &= \alpha(\beta(P)) + \alpha(\gamma(P)) \\ &= (\alpha \circ \beta)(P) + (\alpha \circ \gamma)(P),\end{aligned}$$

所以 $\alpha \circ (\beta + \gamma) = \alpha \circ \beta + \alpha \circ \gamma$. 同理可以证明 $(\alpha + \beta) \circ \gamma = \alpha \circ \gamma + \beta \circ \gamma$.

例 2.2 常值映射和平移映射中只有 $c_O = [0]$ 和 $\tau_O = id$ 是自同态. 对于 $m \in \mathbb{Z}$，定义 m 倍点映射

$$[m] : E \to E$$

$$P \mapsto mP.$$

若 $m > 0$，则 $mP = (m-1)P + P$，所以 $[m] = [m-1] + id$；若 $m < 0$，则 $mP = -((-m)P)$，所以 $[m] = -[-m]$. 由此知 $[m]$ 是有理映射，因为 $m(P+Q) = mP + mQ$，所以 $[m]$ 是自同态.

推论 2.1.6 $\mathrm{End}(E)$ 是 $\mathbb{Z}$ 代数，其中自同态乘以 $m \in \mathbb{Z}$ 定义为自同态与 $[m]$ 的复合.

证明 已知 $\mathrm{End}(E)$ 是环，$\mathbb{Z}$ 是其子环，自然地 $\mathrm{End}(E)$ 是 $\mathbb{Z}$ 模，所以 $\mathrm{End}(E)$ 是 $\mathbb{Z}$ 代数.

定义 2.1.7 如果除 m 倍点映射外，$\mathrm{End}(E)$ 中还有其他元素，则称 E 有复乘.

例 2.3 $\mathbb{C}$ 上椭圆曲线 $E: Y^2 = X^3 + 1$，令 $\omega^3 = 1, \omega \neq 1$，则

$$\alpha : E \to E,$$
$$(x, y) \mapsto (\omega x, y)$$

是自同态. α 显然是有理映射；直接验证 α 具有同态性质.

若基域 $k = \mathbb{F}_q$ 是有限域，则映射 $\varphi = (X^q, Y^q)$，对于 $P = (x, y) \in E$，有

$$E(\varphi(P)) = E(x^q, y^q),$$

注意到 E 定义在 k 上，所以 E 的系数 $a_i = a_i^q$，则

$$E(x^q, y^q) = E(x, y)^q = 0,$$

故 $\varphi(P) \in E$，φ 为有理映射，同理可知

$$\varphi(P+Q) = \varphi(P) + \varphi(Q),$$

即 φ 为自同态，称为 Frobenius 自同态，所以定义在 k 上的椭圆曲线 E 有复乘.

定义 2.1.8 设 m 是整数，P 是 E 上的一个点，则如果 $mP = O$，称 P 为 m 扭点 (m-torsion point). 所有的 m 扭点组成的集合记作 $E[m]$. 点 P 的阶为 m，若 $mP = O$ 且对于 $0 < m' < m$，$m'P \neq O$.

可知 m 扭点恰好是 $[m]$ 的核.

定理 2.1.9 设 m 是非零整数，则 $E[m]$ 是有限群且 $[m] \neq [0]$，因此存在有理函数 g_m, h_m，使得 $[m] = (g_m, h_m)$，g_m, h_m 的极点恰好是 $E[m]$ 中的点.

证明 $[m] \neq [0]$ 等价于 $|E[m]| < \infty$. 如果 $[m] = [0]$，显然 $E[m] = \ker[m] = E$ 是无限群；如果 $[m] \neq [0]$，则存在有理函数 g_m,h_m，使得 $[m] = (g_m, h_m)$，若 $[m](P) = mP = O$，则意味着 P 是 g_m,h_m 的极点. 因为有理函数只有有限个极点，所以 $E[m]$ 是有限群. 故只需证 $[m] \neq [0]$，即得结论. 由于 $E[-m] = E[m]$，所以仅需考虑正整数 m.

(1) 若 $m = 1$，显然 $[1] \neq [0]$.

(2) 若 $m = 2$，则 $[2] \neq [0]$ 当且仅当 $[1] \neq [-1]$，该结论显然成立.

(3) 若 m 是奇素数且 $p \neq 2$，因为 E 有 2 阶点 P，则

$$mP = (m-1)P + P = O + P = P \neq O,$$

故 $[m] \neq [0]$.

(4) 若 m 是奇素数且 $p = 2$. 如果 $j \neq 0$，则 E 有 2 阶点，同上可证 $[m] \neq [0]$；如果 $j = 0$，设 E 为 $Y^2 + a_3Y = X^3 + a_4X + a_6$， $P = (x, y)$，则

$$X(2P) = \frac{x^4 + a_4^2}{a_3^2}$$

如果 P 是 3 阶点，那么 $X(2P) = X(P)$，设 $x \in K$ 满足

$$\frac{x^4 + a_4^2}{a_3^2} = x,$$

$y \in K$ 是 $E(x, Y) = 0$ 的解，则 P 是 3 阶点. 因为至多有 4 个 K 中元素满足 $\frac{x^4 + a_4^2}{a_3^2} = x$，而对于每个 $x, E(x, Y) = 0$ 在 K 中至多有 2 个解，故

$$E[3] = \{(x, y) : x^4 + a_3^2x + a_4^2 = 0, E(x, y) = 0\} \cup \{O\}$$

是有限群. 因此 $[3] \neq [0]$. 如果 $m \neq 3$，则对于 3 阶点 P， $mP \neq O$，所以 $[m] \neq [0]$.

(5) 若 m 是合数，设 d 是 m 的素因子，对于群同态

$$\rho : E[m] \to E[d],$$
$$P \mapsto \frac{m}{d}P.$$

其像集 $\mathrm{im}\rho$ 是 $E[d]$ 的子群，所以是有限群；其核 $\ker\rho$ 为 $E[\frac{m}{d}]$，也是有限群，故

$$|E[m]| = |\mathrm{im}\rho||\ker\rho|$$

有限，即 $[m] \neq [0]$.

推论 2.1.10 如果 $m \neq n$，则 $[m] \neq [n]$.

证明 $[m] = [n]$ 当且仅当 $[m-n] = [0]$，由上述定理可知，当且仅当 $m - n = 0$.

对于 (g_m, h_m)，用加法和倍点公式容易获得递归关系. 显然 $g_1 = X, h_1 = Y$. 因为 $[2] = [1] + [1]$，所以

$$\begin{aligned} g_2 &= -2X + \lambda^2 + a_1\lambda - a_2, \\ h_2 &= -\lambda(g_2 - X) - a_1 g_2 - a_3 - Y, \\ \lambda &= \frac{3X^2 + 2a_2 X + a_4 - a_1 Y}{2Y + a_1 X + a_3}. \end{aligned}$$

如果 $m > 2$，则由推论知 $[m-1] \neq [1]$，则 $[m] = [m-1] + [1]$：

$$\begin{aligned} g_m &= -g_{m-1} - X + \lambda^2 + a_1\lambda - a_2, \\ h_m &= -\lambda(g_m - X) - a_1 g_m - a_3 - Y, \\ \lambda &= \frac{h_{m-1} - Y}{g_{m-1} - X}. \end{aligned}$$

显然，同种一定把无穷远点 O 映射到 O，事实上，该逆命题也成立. 本节只给出特征不为 2 的域的证明. 以下均假设 K 的特征不为 2.

定义 2.1.11 有理映射 α 是偶映射 (奇映射)，若对于任意的 $P \in E$，有 $\alpha(P) = \alpha(-P)$ ($\alpha(-P) = -\alpha(P)$).

偶同种一定是 $[0]$，即将所有的点均映射到 O. 因为非常值有理映射 α 可以分解为移位映射和 α' 的复合，其中 $\alpha'(O) = O$，所以如果将 O 映射到 O 的有理映射是同种，则所有的偶有理映射均是常值映射.

定理 2.1.12 偶有理映射均为常值映射.

证明 设 $\alpha = (\alpha_1, \alpha_2) \in E'(K(E))$ 是偶有理映射. 因为 $\alpha(-P) = \alpha(P)$，所以 $\alpha_1(-P) = \alpha_1(P), \alpha_2(-P) = \alpha_2(P)$，则 $\alpha_1, \alpha_2 \in K(X)$. 又因为 α_1, α_2 满足 E' 的方程，可证明 α_1, α_2 一定有形式

$$\alpha_1 = \frac{a}{c^2}$$

$$\alpha_2 = \frac{b}{c^3}$$

其中， $a,b,c \in K[X]$(见习题 2.2)，且 c 是 α_1,α_2 的上述表示式中次数最低的多项式，即

$$\deg c = \min\{\deg c' : \alpha_1 = a'/c'^2, \alpha_2 = b'/c'^3, a', b', c' \in K[X]\}.$$

不妨设

$$E' : Y^2 = (X - d_1)(X - d_2)(X - d_3)$$

其中， $d_1,d_2,d_3 \in K$ 且互不相同，则

$$b^2 = (a - d_1c^2)(a - d_2c^2)(a - d_3c^2).$$

若 d 是 $a - d_1c^2, a - d_2c^2$ 的公因子且不可约，则 d 整除 a,c^2，所以 d 是 $a - d_3c^2$ 的因子，从而 $d^3|b^2$，则 $d^4|b^2$，故存在 $1 \leqslant i \leqslant 3$ 使得 $d^2|a - d_ic^2$. 因为 $d|c^2,d$ 不可约，所以 $d^2|c^2$，故 $d^2|a$. 由此得 $d^6|b^2$，即 $d^3|b$，则可用 $a/d^2,b/d^3,c/d$ 替换 a,b,c 来表示 α_1,α_2，而 c/d 的次数小于 c 的次数，与 c 的次数极小矛盾，所以 $a - d_1c^2,a - d_2c^2,a - d_3c^2$ 两两互素．故有下式

$$a - d_1c^2 = s_1^2,$$
$$a - d_2c^2 = s_2^2,$$
$$a - d_3c^2 = s_3^2,$$

其中， s_1,s_2,s_3 是两两互素的多项式．通过约化，可知存在非零且互异的 $t_1^2,t_2^2 \in K$，使得

$$s_1^2 - s_3^2 = t_1^2c^2, \tag{2.1}$$

$$s_1^2 - s_2^2 = t_2^2c^2,$$

其中， s_1, s_2, s_3 两两互素．现断言 s_1, s_2, s_3, c 全是常数.

若上式存在不全是常数的解 s_1, s_2, s_3, c 且 s_1, s_2, s_3 两两互素，则取其中 $\max(\deg s_1, \deg s_3)$ 最小的解 s_1, s_2, s_3，因为 s_1, s_3 互素，由式 (2.1) 知存在互素的多项式 f, g, 使得 $s_1 - s_3 = 2f^2, s_1 + s_3 = 2g^2$ 且 f, g 不全是常数 (若 f, g 为常数，则 s_1, s_3 为常数，从而 c 为常数， s_2 为常数), 则

$$2\max(\deg f, \deg g) \leqslant \max(\deg s_1, \deg s_3).$$

由于 f, g 不全为常数，故

$$\max(\deg f, \deg g) < \max(\deg s_1, \deg s_3).$$

再由 $s_1^2 - s_2^2 = t_2^2 c^2$ 得

$$f^4 - \lambda f^2 g^2 + g^4 = s_2^2,$$

其中

$$\lambda = 4(t_2/t_1)^2 - 2 \neq \pm 2.$$

将该式分解得

$$(f^2 - \mu g^2)(f^2 - \mu' g^2) = s_2^2,$$

其中

$$\begin{aligned} \mu\mu' &= 1, \\ \mu + \mu' &= \lambda \neq \pm 2, \end{aligned}$$

故 μ, μ' 不相等且不为 0. 因此存在多项式 h, k, 使得

$$\begin{aligned} f^2 - h^2 &= \mu g^2, \\ f^2 - k^2 &= \mu' g^2 \end{aligned}$$

且 f, k, h 两两互素 (否则， f, g 不互素)，则 $(f, k, h, *)$ 是式 (2.1) 的解，而

$$\max(\deg f, \deg h) \leqslant \max(\deg f, \deg g) < \max(\deg s_1, \deg s_3),$$

矛盾. 故若 $\alpha_1, \alpha_2 \in K(X)$ 满足 E 的方程，则 α_1, α_2 一定是常数，即 α 是常值映射. 结论得证.

定理 2.1.13 设有理映射 $\alpha \in E'(K(E))$ 满足 $\alpha(O) = O$，则 α 是同种映射.

证明 设 α 是奇有理映射，对于 $Q \in E$，定义

$$\beta_Q(P) = \alpha(P + Q) - \alpha(P - Q).$$

显然 $\beta_Q(-P) = \beta_Q(P)$，即 β_Q 是偶映射，则 β_Q 是常值映射，所以对于任意的 $P \in E$ 有

$$\beta_Q(P) = \beta_Q(O) = \alpha(Q) - \alpha(-Q) = 2\alpha(Q).$$

已有 $\alpha(O) = O$ ，设对于小于等于 $n \geqslant 1$ 的非负整数 k 均有 $\alpha(kP) = k\alpha(P)$ ，下证 $\alpha((n+1)P) = (n+1)\alpha(P)$. 因为

$$\begin{aligned}\beta_P(nP) &= \alpha((n+1)P) - \alpha((n-1)P)\\ &= \alpha((n+1)P) - (n-1)\alpha(P)\end{aligned}$$

而 $\beta_P(nP) = 2\alpha(P)$ ，所以

$$\alpha((n+1)P) = 2\alpha(P) + (n-1)\alpha(P) = (n+1)\alpha(P).$$

又因为 α 是奇映射，故对于所有整数 n 具有 $\alpha(nP) = n\alpha(P)$.

令 $\gamma_Q(P) = \alpha(P+Q) - \alpha(P) - \alpha(Q)$ ，设 $mP = Q$ ，则

$$\begin{aligned}\gamma_Q(P) &= \gamma_{mP}(P)\\ &= \alpha(P+mP) - \alpha(P) - \alpha(mP)\\ &= (m+1)\alpha(P) - \alpha(P) - m\alpha(P)\\ &= O\end{aligned}$$

因此，对于任意给定的 Q ，若 $P \in E$ 且存在整数 m，使得 $mP = Q$ ，则 $\gamma_Q(P) = O$ ，由定理 2.5.3 知存在无穷多的 P，使得 $\gamma_Q(P) = O$ ，所以 $\gamma_Q = [0]$ ，即 α 是同种.

设 α 是有理映射. 令 $\alpha_\pm \in E'(K(E))$ 为

$$\begin{aligned}\alpha_+(P) &= \alpha(P) + \alpha(-P),\\ \alpha_-(P) &= \alpha(P) - \alpha(-P),\end{aligned}$$

其中， $P \in E$ ，则 $2\alpha = \alpha_+ + \alpha_-$. 因为 $\alpha_+(-P) = \alpha_+(P)$ ，即 α_+ 是偶有理映射，且 $\alpha_+(O) = O$ ，所以对于任意的 $P \in E$，有 $\alpha_+(P) = O$ ，故 $2\alpha = \alpha_-$. 因为 α_- 是奇有理映射且 $\alpha_-(O) = O$ ，所以 α_- 是同种，则对于任意的 $P, Q \in E$ ，有

$$2(\alpha(P+Q) - \alpha(P) - \alpha(Q)) = O,$$

即 $\alpha(P+Q) - \alpha(P) - \alpha(Q) \in E'[2]$ ，固定 Q ，则 $\alpha(Q+\cdot) - \alpha(\cdot) - \alpha(Q)$ 是不满的有理映射，所以该有理映射是常值映射，而 $\alpha(O) = O$ ，则 $\alpha(P+Q) = \alpha(P) + \alpha(Q)$. 结论得证.

实际上，对于特征为 2 的域，该结论也成立．由于其证明涉及内容较多，故略去，有兴趣的读者可以参看文献 [126].

2.2 同种的次数

对于任意有理映射 $\alpha \in E'(K(E))$ 可以自然地诱导出映射：

$$\alpha^* : K(E') \to K(E),$$
$$r \mapsto r \circ \alpha.$$

本节主要研究 α^* 的相关性质.

命题 2.2.1 如果 α 是非常值有理映射，则 α^* 是域的单同态.

证明 显然 α^* 是域同态．如果 $r \circ \alpha = s \circ \alpha$ ， $r, s \in K(E')$ ，则对于任意的 $P \in E$ ，有 $r(\alpha(P)) = s(\alpha(P))$ ，因为 α 不是常值映射，所以当 P 跑遍 E 时， $\alpha(P)$ 也跑遍 E' ，即对于任意的 $Q \in E'$ 有 $r(Q) = s(Q)$ ，所以 $r = s$.

给定点 $P \in E$ ，设 u 是 $\alpha(P)$ 的一致性参数，因为 u 在 $\alpha(P)$ 的赋值为 1 ，所以 P 是 $\alpha^*(u) = u \circ \alpha$ 的零点.

定义 2.2.2 设 $\alpha \in E'(K(E))$ 是非常值有理映射， $P \in E, u$ 是 $\alpha(P)$ 的一致性参数，则称

$$e_\alpha(P) = \mathrm{ord}_P(u \circ \alpha)$$

为 α 在 P 的分歧指数 (ramification index). 如果 $e_\alpha(P) > 1$ ，称 α 在 P 分歧；否则，称 α 在 P 非分歧．如果 α 在 E 的任意点均非分歧，则称 α 是非分歧的.

因为 P 是 $u \circ \alpha$ 的零点，所以分歧指数 $e_\alpha(P) \geqslant 1$. 分歧指数不依赖于 u 的选择．设 u' 是 $\alpha(P)$ 的另一个一致性参数，则 $\frac{u'}{u}$ 在 $\alpha(P)$ 正则，且 $\alpha(P)$ 不是其零点，即 $\frac{u'}{u} \circ \alpha$ 在 P 正则，且 P 不是其零点，故

$$\begin{aligned}
\mathrm{ord}_P(u' \circ \alpha) &= \mathrm{ord}_P((u\frac{u'}{u}) \circ \alpha) \\
&= \mathrm{ord}_P(u \circ \alpha) + \mathrm{ord}_P(\frac{u'}{u} \circ \alpha) \\
&= \mathrm{ord}_P(u \circ \alpha).
\end{aligned}$$

因为非零有理函数只有有限个零点，所以对于给定的点 $Q \in E'$ ，仅有有限个点 $P \in E$, 使得 $\alpha(P) = Q$. 故可由 α 诱导出如下除子群之间的同态，在不引起

混淆时也将此同态记作 α^*:

$$\begin{aligned}\alpha^* : \mathrm{Div}(E') &\to \mathrm{Div}(E)\\ <Q> &\mapsto \sum_{P\in\alpha^{-1}(Q)} e_\alpha(P) <P>.\end{aligned}$$

引理 2.2.3 设 $\alpha \in E'(K(E))$ 是非常值有理映射，$r \in K(E')$，$P \in E$，则 $\mathrm{ord}_P(r\circ\alpha) = e_\alpha(P)\mathrm{ord}_{\alpha(P)}(r)$.

证明 设 u 是 $\alpha(P)$ 的一致性参数，当 $r = u$ 时，由分歧指数定义知结论成立. 设 $r = u^d r_1$，r_1 是在 $\alpha(P)$ 正则的有理函数，且 $\alpha(P)$ 不是其零点，即 $d = \mathrm{ord}_{\alpha(P)}(r)$，则

$$\begin{aligned}\mathrm{ord}_P(r\circ\alpha) &= d\,\mathrm{ord}_P(u\circ\alpha) + \mathrm{ord}_P(r_1\circ\alpha)\\ &= d\,e_\alpha(P).\end{aligned}$$

命题 2.2.4 对于非常值有理映射 $\alpha \in E'(K(E))$，下图可交换

$$\begin{array}{ccc} K(E'),\ r & \xrightarrow{\alpha^*} & K(E),\ r\circ\alpha \\ \downarrow{\scriptstyle \mathrm{div}} & & \downarrow{\scriptstyle \mathrm{div}} \\ \mathrm{Div}(E'),\ \mathrm{div}\ r & \xrightarrow{\alpha^*} & \mathrm{Div}(E),\ \mathrm{div}(r\circ\alpha). \end{array}$$

证明

$$\begin{aligned}\mathrm{div}(r\circ\alpha) &= \sum_{P\in E} \mathrm{ord}_P(r\circ\alpha) <P>\\ &= \sum_{P\in E} e_\alpha(P)\mathrm{ord}_{\alpha(P)}(r) <P>\\ &= \sum_{Q\in E'} \mathrm{ord}_Q(r) \sum_{P\in\alpha^{-1}(Q)} e_\alpha(P) <P>\\ &= \sum_{Q\in E'} \mathrm{ord}_Q(r)\alpha^*(<Q>)\\ &= \alpha^*(\sum_{Q\in E'} \mathrm{ord}_Q(r) <Q>)\\ &= \alpha^*(\mathrm{div}\ r).\end{aligned}$$

命题 2.2.5 设 E, E', E'' 均是 K 上椭圆曲线，$\alpha \in E'(K\ (E)), \beta \in E''(K(E'))$，则 $\beta \circ \alpha \in E''(K(E))$ 也是非常值有理映射，且

$$\begin{aligned} &e_{\beta\circ\alpha}(P) = e_\alpha(P)e_\beta(\alpha(P)), \qquad \forall P \in E \\ &(\beta \circ \alpha)^* = \alpha^* \circ \beta^* \end{aligned}$$

证明 因为 α, β 是满映射, 所以 $\beta\circ\alpha$ 一定非常值. 设 $P \in E$,u 是 $(\beta\circ\alpha)(P)$ 的一致性参数，则

$$\begin{aligned} e_{\beta\circ\alpha}(P) &= \mathrm{ord}_P((u\circ\beta)\circ\alpha) \\ &= e_\alpha(P)\mathrm{ord}_{\alpha(P)}(u\circ\beta) \\ &= e_\alpha(P)e_\beta(\alpha(P)). \end{aligned}$$

设 $Q \in E''$，则

$$\begin{aligned} (\beta\circ\alpha)^*(< Q >) &= \sum_{P\in(\beta\circ\alpha)^{-1}(Q)} e_{\beta\circ\alpha}(P) < P > \\ &= \sum_{P\in(\beta\circ\alpha)^{-1}(Q)} e_\beta(\alpha(P))e_\alpha(P) < P > \\ &= \sum_{R\in\beta^{-1}(Q)} e_\beta(R) \sum_{P\in\alpha^{-1}(R)} e_\alpha(P) < P > \\ &= \sum_{R\in\beta^{-1}(Q)} e_\beta(R)\alpha^*(< R >) \\ &= \alpha^*\left(\sum_{R\in\beta^{-1}(Q)} e_\beta(R) < R >\right) \\ &= \alpha^*\circ\beta^*(< Q >). \end{aligned}$$

引理 2.2.6 对于 $Q \in E$，映射 τ_Q 是非分歧的.

证明 τ_Q 的逆映射为 τ_{-Q}. 因为对于任意的 $P \in E$，

$$1 = e_{\mathrm{id}}(P) = e_{\tau_{-Q}\circ\tau_Q}(P) = e_{\tau_Q}(P)e_{\tau_{-Q}}(P+Q).$$

$e_{\tau_Q}(P) \geqslant 1, e_{\tau_{-Q}}(P+Q) \geqslant 1$，所以 $e_{\tau_Q}(P) = 1$.

定理 2.2.7 设 $\alpha \in E'(K(E))$ 是非零同种，则 $e_\alpha(P)$ 与 $P \in E$ 的选取无关. 以后常记作 e_α.

证明 设 $P\in E$，对于任意的 $Q\in E$， $\alpha(P+Q)=\alpha(P)+\alpha(Q)$，所以 $\alpha\circ\tau_P=\tau_{\alpha(P)}\circ\alpha$，则

$$\begin{aligned}e_\alpha(P)&=\frac{e_{\alpha\circ\tau_P}(O)}{e_{\tau_P}(O)}\\&=e_{\alpha\circ\tau_P}(O)\\&=e_{\tau_{\alpha(P)}\circ\alpha}(O)\\&=e_\alpha(O)e_{\tau_{\alpha(P)}}(\alpha(O))\\&=e_\alpha(O).\end{aligned}$$

推论 2.2.8 设 $\alpha\in E'(K(E)),\beta\in E''(K(E'))$ 是非零同种，则 $e_{\beta\circ\alpha}=e_\alpha e_\beta$.

对于 $k=\mathbb{F}_q$ 上的 Frobenius 自同态 φ 有结论：

命题 2.2.9 $e_\varphi=q$.

证明 已知 $\dfrac{X}{Y}$ 是 $O=\varphi(O)$ 的一致性参数，则

$$e_\varphi=e_\varphi(O)=\mathrm{ord}_O\left(\frac{X}{Y}\circ\varphi\right)=\mathrm{ord}_O((\frac{X}{Y})^q)=q.$$

引理 2.2.10 设 $k(x),k(y)$ 均是单变量有理函数域， $L/k(x),J/k(y)$ 均是有限的域扩张，若 $J\subseteq L$，则 L/J 也是有限扩张.

证明 因为 $[L:k(x)]$ 有限且 $y\in J\subseteq L$，所以 $[L:k(x,y)]$ 有限，y 是 $k(x)$ 的代数元，故 $[k(x,y):k(x)]$ 有限，又因为 $k(x)\cong k(y)$，所以 $[k(x,y):k(y)]$ 有限， $[L:k(y)]=[L:J][J:k(y)]$ 有限，即得 $[L:J]$ 有限.

α^* 的像集是 $K(E)$ 的子域，因为 $K(E),\alpha^*(K(E'))$ 相对于 K 的超越次数均为 1，且 $[K(E):K(X)]<\infty$，所以由引理 2.2.10 可知域扩张 $K(E)/\alpha^*(K(E'))$ 是有限扩张.

定义 2.2.11 非零同种 $\alpha\in E'(K(E))$ 所确定的域扩张 $K(E)/\alpha^*(K(E'))$ 的次数 (可分次数、不可分次数) 分别称为 α 的次数 (可分次数，不可分次数)，分别记作 $\deg\alpha(\deg_s\alpha,\deg_i\alpha)$.

定义 2.2.12 对于同种 $\alpha\in E'(K(E))$，若存在同种 $\beta\in E(K(E'))$ 满足 $\alpha\circ\beta=\mathrm{id}|_{E'},\beta\circ\alpha=\mathrm{id}|_E$，则称 α 为同构，记 $\beta=\alpha^{-1}$.

为描述方便，以后本节所述的结论仅给出特征不为 2 时的证明，若 K 的特征为 2，证明请见文献 [126].

设 $E: Y^2 = X^3 + a_2X^2 + a_4X + a_6, E': Y'^2 = X'^3 + a_2'X'^2 + a_4'X' + a_6'$ 是 K 上的椭圆曲线， $\alpha \in E'(K(E))$ 是非零同种， $K' = \alpha^*(K(E'))$. 显然 $K' \subset K(E)$.

令 $\mathcal{S} = \ker\alpha \subset E$ ， $T_{\mathcal{S}} = \{\tau_P : P \in \mathcal{S}\}$, 则 $T_{\mathcal{S}}$ 在加法意义下构成 $\mathrm{End}(E)$ 的一个有限子群. $T_{\mathcal{S}}$ 对 $K(E)$ 的作用定义为

$$\tau_P(r) = \tau_P^*(r) = r \circ \tau_P.$$

若 $r \in K'$ ，则存在 $r' \in K(E')$, 使得 $r = r' \circ \alpha$ ，对于任意的 $Q \in E$ 有

$$[\tau_P(r)](Q) = r'(\alpha(Q+P)) = r'(\alpha(Q)) = r(Q),$$

即 $T_{\mathcal{S}}$ 保持 K' 不动. 令

$$L = \{r \in K(E) : \tau_P(r) = r, \forall P \in \mathcal{S}\},$$

由域论知 $K(E)$ 是 L 的 Galois 扩张，其扩张次数 $m = |\mathcal{S}|$.

令 $\tilde{X} = [\mathrm{Tr}_{K(E)/L}](X), \tilde{Y} = [\mathrm{Tr}_{K(E)/L}](Y)$ ，则

$$\tilde{X} = \sum_{P \in \mathcal{S}} \tau_P(X),$$
$$\tilde{Y} = \sum_{P \in \mathcal{S}} \tau_P(Y),$$

且 $\tilde{X}, \tilde{Y}$ 以 $\mathcal{S}$ 中的点为 2 重、 3 重极点，此外，无其他极点.

命题 2.2.13 $\tilde{X}, \tilde{Y}$ 生成 L.

证明 显然 $\tilde{X}, \tilde{Y} \in L$. 设 $r \in L$ 且是偶函数，即对于任意的 $P \in E$ ，有 $r(-P) = r(P)$ ， r 乘以

$$\prod_{P \notin \mathcal{S}, r(P) = O} (\tilde{X} - \tilde{X}(P))$$

的适当幂次，可以获得 L 中的偶有理函数 r_1 ，且 r_1 的极点均属于 $\mathcal{S}$. r_1 是偶函数，则 $\mathrm{ord}_O(r_1)$ 是偶数，设 $\mathrm{ord}_O(r_1) = -2t, t \geqslant 0. r_1$ 减去 $\tilde{X}^t$ 的适当倍数，可以得到 L 中的一个偶函数，其极点均属于 $\mathcal{S}$ 且 O 的重数至多为 $2t-2$ ；重复该步骤，则最终可得

$$r_1 = p(\tilde{X}) + g.$$

其中，p 是多项式，偶函数 $g \in L$ 的极点均属于 $\mathcal{S} \setminus \{O\}$ 且 $g(O) = 0$. 由 $g \in L$ 可知，对于任意的 $P \in \mathcal{S}$ 有 $g(P) = g(O) = 0$，所以 g 没有极点，即 $g = 0$，则 $r_1 \in K[\tilde{X}], r \in K(\tilde{X})$. 若 $r \in L$ 是奇函数，则 $\tilde{Y}r$ 是偶函数，故 $\tilde{Y}r \in K(\tilde{X})$，即 $r \in K(\tilde{X}, \tilde{Y})$. 又因为任意有理函数均可以表示为一个奇函数和一个偶函数的和，而 L 中的奇函数和偶函数均属于 $K(\tilde{X}, \tilde{Y})$，所以 L 由 $\tilde{X}, \tilde{Y}$ 生成. 结论得证.

定理 2.2.14 设非零同种 $\alpha \in E'(K(E))$，$\mathcal{S} = \ker \alpha$，$L = \{r \in K(E) : \tau_P(r) = r, \forall P \in S\}$，则存在椭圆曲线 C 使得：

(1) $K(C)$ 同构于 L;

(2) 且存在同种 $\beta \in C(K(E)), \gamma \in E'(K(C))$ 满足：

① $\alpha = \gamma \circ \beta$,

② $\ker \beta = \ker \alpha$,

③ $\ker \gamma = \{\tilde{O}\}$, 其中 $\tilde{O}$ 是 C 的零元,

④ $e_\beta = 1$,

⑤ $e_\gamma = e_\alpha$.

证明 因为 $\tilde{Y}^2$ 是偶函数，且 $\tilde{Y}^2$ 的所有极点均属于 $\mathcal{S}$，则由命题 2.2.13 的证明过程知 $\tilde{Y}^2 \in K[\tilde{X}]$，而 $\mathrm{ord}_O(\tilde{Y}^2) = -6, \mathrm{ord}_O(\tilde{X}) = -2$，所以存在三次多项式 $f(\tilde{X}) \in K[\tilde{X}]$ 使得

$$\tilde{Y}^2 = f(\tilde{X}).$$

取 $k \in K$ 使得 $f(k) = 0$，令 $N = |\{P \in E : \tilde{X}(P) = k\}|$，由 $\tilde{X}(P) = k$ 可知 $\tilde{Y}(P) = 0$. 因此，如果对于 $P, Q \in E, \tilde{X}(P) = \tilde{X}(Q) = k$，则 $\tilde{Y}(P) = \tilde{Y}(Q) = 0$，又因为 $K' \subset L = K(\tilde{X}, \tilde{Y})$，所以对于 $\tilde{X}(P) = k$ 的任意点 $P \in E$, 有相同的 $\alpha(P)$，即 α 将 E 的 N 个点映射到 E' 的同一个点，故 $N \leqslant |\ker \alpha|$. 另一方面，$\tilde{X}$ 在 $T_{\mathcal{S}}$ 作用下不动，所以对于任意的 $Q \in \mathcal{S}, P \in E$ 有 $\tilde{X}(P+Q) = \tilde{X}(P)$，即至少有 $|\mathcal{S}|$ 个 $P \in E$ 使得 $\tilde{X}(P) = k$，亦即 $N \geqslant |\ker \alpha|$，所以 $N = |\ker \alpha|$.

令集合 $\mathcal{R} = \{P \in E : \tilde{Y}(P) = 0\}$. 若 $\tilde{Y}(P) = 0$，则存在 f 的某个根 k 使得 $\tilde{X}(P) = k$. 设 f 有 M 个不同的根，则 $|\mathcal{R}| = M \cdot |\ker \alpha|$，即有 $M \cdot |\ker \alpha|$ 个 E 中的点为 $\tilde{Y}$ 的零点.

因为 α 是满映射，所以存在 $P \in E$ 使得 $2\alpha(P) = O'$ 且 $\alpha(P) \neq O'$. 设集合

$$P + \mathcal{S} = \{P + Q : Q \in \mathcal{S}\},$$

对于 $P+Q\in P+\mathcal{S}$，有 $-(P+Q)=P+R, R=-2P-Q$，而

$$\alpha(R)=-2\alpha(P)-\alpha(Q)=O',$$

故 $R\in\mathcal{S}$， $-(P+Q)\in P+\mathcal{S}$，又因为

$$\tilde{Y}(P)=\sum_{Q\in\mathcal{S}}Y(P+Q),$$
$$Y(-(P+Q))=-Y(P+Q),$$

所以对于任意的 $P\in E$，若 $\alpha(P)\in E'[2]\setminus\{O'\}$，则 $\tilde{Y}(P)=0.$

由 α 是满映射，可知对于 E' 中的任意点，均有 E 中的 $|\ker\alpha|$ 个点是其原像，而 $E'[2]$ 中有三个有限点，所以至少有 $3|\ker\alpha|$ 个点是 $\tilde{Y}$ 的零点 0，则 $M\geqslant 3$，已知 f 次数为 3，所以 $M=3$，即 f 有三个不同的根， $\tilde{Y}^2=f(\tilde{X})$ 决定了一条椭圆曲线，记作 C. 则由命题 2.2.13 知 $K(C)$ 同构于 L. 结论 1 得证.

若 $\tilde{X}(P)=\tilde{X}(Q),\tilde{Y}(P)=\tilde{Y}(Q)$，则 $P-Q\in\mathcal{S}$，因此 C 可以看作商群 $E/\mathcal{S}$. 定义同种

$$\begin{aligned}\beta:E&\longrightarrow C\\ P&\longmapsto(\tilde{X}(P),\tilde{Y}(P))\end{aligned}$$

令 $\bar{X}=X'\circ\alpha,\bar{Y}=Y'\circ\alpha$，则 $\bar{X},\bar{Y}\in L=K(C)$，定义同种

$$\begin{aligned}\gamma:C&\longrightarrow E'\\ \tilde{P}&\longmapsto(\bar{X}(P),\bar{Y}(P))\end{aligned}$$

其中， $\tilde{P}=\beta(P)$. 因为 $\alpha(P)=(\bar{X}(P),\bar{Y}(P))$，所以 $\alpha=\gamma\circ\beta$.

由 $C=E/\mathcal{S}$，易得②、③.

因为 $e_\beta=e_\beta(O)=\mathrm{ord}_O\left(\frac{X}{Y}\circ\beta\right)=\mathrm{ord}_O\left(\frac{\tilde{X}}{\tilde{Y}}\right)=1$，所以 $e_\alpha=e_\gamma$. 结论证毕.

由定理 2.2.14 可知, 同种 $\alpha\in E'(K(E))$ 可以分解为同种 $\beta\in C(K(E)),\gamma\in E'(K(C))$ 的复合，其中 β 的分歧指数为 1， γ 是单映射，且

$$\beta^*(K(C))=L,$$
$$\beta^*(\gamma^*(K(E')))=K',$$
$$[K(C):\gamma^*(K(E'))]=[\beta^*(K(C)):K'].$$

命题 2.2.15 设同种 $\alpha \in E'(K(E))$ 是单映射, 则 α 是同构当且仅当 $e_\alpha = 1$ 或 $K(E)$ 是 K' 的可分扩张.

证明 设 $\bar{X} = \alpha^*(X'), \bar{Y} = \alpha^*(Y')$，其中 X', Y' 是 E' 的坐标函数. 因为 $\bar{X}$ 是偶函数, $\bar{X} \in K' = \alpha^*(K(E')) \subset K(X,Y)$，所以 $\bar{X} \in K(X)$. 又因为 $\bar{X}$ 非常值, 故对任意 $k \in K$ 一定存在 $l \in K$ 使得 $\bar{X}(l) = k$. 现断言上述的 l 是唯一的.

如果存在 $l, l' \in K$, 使得 $\bar{X}(l) = \bar{X}(l')$. 设 $P, Q \in E, X(P) = l, X(Q) = l'$，则

$$\alpha(P) = (\bar{X}(P), \bar{Y}(P)) = (\bar{X}(Q), \pm\bar{Y}(Q)) = \pm\alpha(Q).$$

又因为 $X(-Q) = X(Q) = l'$，故不妨设 $\alpha(P) = \alpha(Q)$，则与已知 α 是单映射矛盾.

由 α 是单映射, 可知 $\bar{X}$ 没有有限极点, 故 $\bar{X} \in K[X]$. 而 $\bar{X}$ 的像集为整个 K 且原像唯一, 所以存在 $a \neq 0, b \in K, r \geqslant 0$，使得 $\bar{X} = (aX+b)^{p^r}$，其中 p 是 K 的特征. 故 $aX + b$ 是 $Z^{p^r} - \bar{X} \in K'[Z]$ 的根. 若 $\bar{X} = \alpha^*(X')$ 在 K' 有 p 次根, 则 X' 在 $K(E')$ 有 p 次根, 矛盾, 所以 $Z^{p^r} - \bar{X}$ 不可约 (见习题 2.3)，即 $Z^{p^r} - \bar{X}$ 是 $aX + b$ 的极小多项式, 则 $K(E)/K'$ 可分当且仅当 $r = 0$. 又因为 $\mathrm{ord}_O(\bar{X}) = -2e_\alpha$，所以 $e_\alpha = p^r$，则 $K(E)/K'$ 可分当且仅当 $e_\alpha = 1$.

如果 α 是同构的, 显然有 $e_\alpha = 1$. 若 $e_\alpha = 1$，由 $\bar{X} = aX + b \in K'$ 知 $X \in K'$. 因为 α 是单映射, 所以 $\bar{Y}$ 没有有限极点, 又因为 $\bar{Y}$ 是奇函数, 故存在 $h \in K[X]$，使得 $\bar{Y} = Yh$. 因为 $e_\alpha = 1$，所以 $\mathrm{ord}_O(\bar{X}) = -2, \mathrm{ord}_O(\bar{Y}) = -3$，而 $\mathrm{ord}_O(\bar{Y}) = \mathrm{ord}_O(Y) + \mathrm{ord}_O(h) = -3 + \mathrm{ord}_O(h)$，故 $\mathrm{ord}_O(h) = 0$，则 h 是非零常数. 所以

$$\alpha = (aX + b, hY);$$
$$\alpha^{-1} = ((a^{-1}(\bar{X} - b), h^{-1}\bar{Y}).$$

结论证毕.

推论 2.2.16 设非零同种 $\alpha \in E'(K(E))$，则 $e_\alpha = 1$ 当且仅当 $K(E)$ 是 K' 的可分扩张.

证明 由定理 2.2.14 知 $\alpha = \gamma \circ \beta$，且 $e_\gamma = e_\alpha, e_\beta = 1$. 则 $e_\alpha = 1$ 当且仅当 $e_\gamma = 1$，因为 γ 是单映射, 由上述命题知 $e_\gamma = 1$ 当且仅当 γ 是同构. 又因为 $K(E)$ 是 $K(C) = L$ 的 Galois 扩张, $e_\beta = 1$，所以 $K(E)$ 是 K' 可分扩张, 当

且仅当 $e_\alpha = 1$. 结论证毕.

推论 2.2.17 设同种 $\alpha \in E'(K(E))$ 是单映射, 则通过适当的坐标变换有 $\alpha(X,Y) = (X^{p^r}, Y^{p^r})$, $e_\alpha = p^r, r \geqslant 0$.

证明 由命题 2.2.15 的证明过程知, 通过适当的坐标变换, 有 $\bar{X} = X' \circ \alpha = X^{p^r}$. 因为 $\bar{Y}$ 是奇函数, 则存在 $h \in K(X)$ 使得 $\bar{Y} = Yh$. 又因为 h 没有有限极点, 故 $h \in K[X]$. 再由 $\bar{Y}^2 = \bar{X}^3 + a_2'\bar{X}^2 + a_4'\bar{X} + a_6'$ 得

$$
\begin{aligned}
Y^2h^2 &= X^{3p^r} + a_2'X^{2p^r} + a_4'X^{p^r} + a_6' \\
&= s(X)^{p^r} + (a_2' - a_2^{p^r})X^{2p^r} + (a_4' - a_4^{p^r})X^{p^r} + (a_6' - a_6^{p^r}),
\end{aligned}
$$

其中, $s(X) = X^3 + a_2X^2 + a_4X + a_6$. 而 $Y^2 = s(X)$, 故 s 整除

$$
B^{p^r}X^{2p^r} + C^{p^r}X^{p^r} + D^{p^r} = (BX^2 + CX + D)^{p^r},
$$

其中 $a_2' - a_2^{p^r} = B^{p^r}, a_4' - a_4^{p^r} = C^{p^r}, a_6' - a_6^{p^r} = D^{p^r}$, 因此 s 整除 $BX^2 + CX + D$, 则 $B = C = D = 0$, 即 $\bar{Y} = Y^{p^r}$, $\alpha(X,Y) = (X^{p^r}, Y^{p^r})$, 由定义知 $e_\alpha = p^r$. 结论证毕.

定理 2.2.18 对于非零同种 $\alpha \in E'(K(E))$, 令 $K' = \alpha^*(K(E')) \subset K(E)$, $N = N_{K(E)/K'}, r \in K(E)$, 则对于任意的 $P \in E$ 有

$$
[N(r)](P) = \prod_{\alpha(Q)=\alpha(P)} r(Q)^{e_\alpha}.
$$

证明 因为 $\alpha = \gamma \circ \beta$, $e_\beta = 1$, $K(E)$ 是 $\beta^*(K(C)) = L$ 的 Galois 扩张, 故 $K(E)/\beta^*(K(C))$ 的 Galois 群为 T_S. 再由推论 2.2.17 知 $\gamma = (\tilde{X}^{p^r}, \tilde{Y}^{p^r})$, $e_\gamma = p^r = e_\alpha$, 故 $[\beta^*(K(C)) : K'] = e_\alpha$, 则

$$
\begin{aligned}
[N(r)](P) &= [N_{\beta^*(K(C))/K'}(N_{K(E)/\beta^*(K(C))}(r))](P) \\
&= \left[N_{\beta^*(K(C))/K'}\left(\prod_{\alpha(Q)=O}(r \circ \tau_Q)\right)\right](P) \\
&= \left[\prod_{\alpha(Q)=O}(r \circ \tau_Q)^{e_\alpha}\right](P) \\
&= \prod_{\alpha(Q)=O} r(P+Q)^{e_\alpha} \\
&= \prod_{\alpha(Q)=\alpha(P)} r(Q)^{e_\alpha}.
\end{aligned}
$$

定理 2.2.19 对非零同种 $\alpha \in E'(K(E))$ 有 $\deg\alpha = e_\alpha|\ker\alpha|$.

证明 若 K 的特征不为 2，由上述定理的证明过程以及 $\deg\alpha = [K(E):K']$ 即得结论. 若 K 的特征为 2，证明请见文献 [126].

例 2.4 对于有限点 $P=(x,y)\in E_*$，$\varphi(P)=(x^q,y^q)$ 一定仍是有限点，所以 $\ker\varphi=\{O\}$，已证 $e_\varphi=q$，故 $\deg\varphi=q$. 令 $J=\varphi^*(K(E))$，由于 $K(E)$ 在 K 上添加了 X,Y，φ^* 保持 K 不动，所以 J 在 K 上添加了 X^q,Y^q，是 $K[X^q,Y^q]/(E)$ 的分式域，所以 $K(E)=J(X,Y)$. 如果 $p\neq 2$，不妨设 $E: Y^2=X^3+a_2X^2+a_4X+a_6$，则

$$Y=\frac{(Y^2)^{\frac{q+1}{2}}}{Y^q}=\frac{(X^3+a_2X^2+a_4X+a_6)^{\frac{q+1}{2}}}{Y^q}\in J(X)$$

所以 $K(E)=J(X)$. 如果 $q=2^m$，则

$$Y=\frac{X^3+a_2X^2+a_4X+a_6+Y^2}{a_1X+a_3}\in J(X,Y^2),$$

所以 $K(E)=J(X,Y)=J(X,Y^2)=J(X,Y^4)=\cdots=J(X,Y^q)=J(X)$. 而 X 是不可约多项式 $T^q-X^q\in J[T]$ 的根，故 $[K(E):J]=q=\deg\varphi$. 因为该不可约多项式是不可分的，所以 $K(E)/J$ 是纯不可分的，与 $|\ker\varphi|=1$ 相一致.

命题 2.2.20 设 $D\in \mathrm{Div}(E'')$，$\alpha\in E''(K(E')),\beta\in E'(K(E))$ 是非零自同态，则

(1) $\deg(\alpha^*(D))=\deg\alpha\deg D$;

(2) $\deg(\alpha\circ\beta)=\deg\alpha\deg\beta$.

证明 由 α^* 和除子的性质知，只需证明对于除子 $D=<Q>$ 结论成立，其中 $Q\in E''$.

$$\begin{aligned}\deg(\alpha^*(D)) &= \deg\left(e_\alpha\sum_{P\in\alpha^{-1}(Q)}<P>\right)\\ &= e_\alpha|\alpha^{-1}(Q)|\\ &= e_\alpha|\ker\alpha|\\ &= \deg\alpha;\end{aligned}$$

$$\deg(\alpha\circ\beta)=e_{\alpha\circ\beta}|\ker(\alpha\circ\beta)|$$

$$= e_\alpha e_\beta |\{P \in E : \beta(P) \in \ker \alpha\}|$$
$$= e_\alpha e_\beta |\ker \alpha||\ker \beta|$$
$$= \deg \alpha \deg \beta.$$

设 $\phi \in E'(K(E))$ 是非常值同种，则

$$\phi^* : \mathrm{Div}(E') \to \mathrm{Div}(E)$$

将零次除子映射到零次除子，故有

$$\phi^* : \mathrm{Pic}^0(E') \to \mathrm{Pic}^0(E).$$

对于 $Q \in E'$，设 $P \in E, \phi(P) = Q$,

$$E' \xrightarrow{f} \mathrm{Pic}^0(E') \xrightarrow{\phi^*} \mathrm{Pic}^0(E) \xrightarrow{f^{-1}} E$$

则

$$f^{-1} \circ \phi^* \circ f(Q) = \deg \phi(P).$$

故有以下定义：

定义 2.2.21 设同种 $\phi \in E'(K(E))$ 且 $\phi \neq 0$，定义 ϕ 的对偶同种为 $\hat{\phi} : E' \to E$, 使得 $\hat{\phi} \circ \phi = \deg \phi$. 若 $\phi = 0$，定义 $\hat{\phi} = 0$.

定理 2.2.22 设 $\phi \in E'(K(E))$ 且 $\phi \neq 0, \deg \phi = m$，则：

(1) 若 ϕ 存在对偶同种，则必唯一.

(2) 作为群同态，$\hat{\phi}$ 等于如下映射的复合：

$$\begin{array}{ccccccc} E' & \xrightarrow{f} & \mathrm{Div}^0(E') & \xrightarrow{\phi^*} & \mathrm{Div}^0(E) & \xrightarrow{\mathrm{sum}} & E \\ Q & \longrightarrow & <Q> - <O> & & \sum n_P <P> & \longrightarrow & \sum n_P P \end{array}$$

证明 (1) 首先证明唯一性. 设 $\hat{\phi}, \hat{\phi}'$ 均为 ϕ 的对偶同种，则

$$(\hat{\phi} - \hat{\phi}') \circ \phi = m - m = 0.$$

因为 $\phi \neq 0$，所以 ϕ 是满映射，故 $\hat{\phi} - \hat{\phi}' = 0$，即 $\hat{\phi} = \hat{\phi}'$.

(2) 设 $Q \in E'$，则

$$\mathrm{sum}\{\phi^*(<Q> - <O>)\} = \sum_{P \in \phi^{-1}(Q)} e_\phi P - \sum_{T \in \phi^{-1}(O)} e_\phi T$$

$$= e_\phi \left(\sum_{P \in \phi^{-1}(Q)} P - \sum_{T \in \phi^{-1}(O)} T \right)$$
$$= e_\phi \circ |\ker \phi| P, \quad P \in \phi^{-1}(Q)$$
$$= \deg \phi P$$

而

$$\hat{\phi}(Q) = \hat{\phi} \circ \phi(P) = \deg \phi P,$$

所以 $\hat{\phi} = \mathrm{sum} \circ \phi^* \circ f$.

实际可以严格证明任意同种必存在唯一的对偶同种，但由于其证明超出了本书的范围，故略去，读者可参看文献 [126]. 由对偶同种的定义，易得以下结论.

定理 2.2.23　设同种 $\phi \in E'(K(E))$，

(1) 设 $m = \deg \phi$，则 $\hat{\phi} \circ \phi = \phi \circ \hat{\phi} = m$.

(2) 设同种 $\psi \in E''(K(E'))$，则 $\widehat{\psi \circ \phi} = \hat{\phi} \circ \hat{\psi}$.

(3) 对于 $m \in \mathbb{Z}$，有 $\hat{m} = m, \deg m = m^2$.

(4) $\deg \hat{\phi} = \deg \phi$.

(5) $\hat{\hat{\phi}} = \phi$.

由于下面重点研究的是映射 $[m]$ 和 m 扭点 $E[m]$，特别是分歧指数 $e_{[m]}$ 的应用，故若对 α 无特殊声明，均是指自同态.

2.3　$K(E)$ 的导数

$K(X)$ 上的导数可以用于研究有理函数的根重数，本节将在 $K(E)$ 上定义具有相同作用的导数的概念.

定义 2.3.1　设 L 是 K 代数，L 上的导数 (derivative) 是一个 K 线性映射 $D: L \to L$，且满足乘积法则：$D(fg) = fDg + gDf$.

令 $f = g = 1$，则 $D1 = 2D1$，所以 $D1 = 0$. 对于任意的常数 $c \in K$，有 $Dc = cD1 = 0$. 若 g 是 L 的单位，令 $f = \dfrac{1}{g}$，则

$$0 = D1 = D\left(g\frac{1}{g}\right) = gD\frac{1}{g} + \frac{Dg}{g},$$

$$D\frac{1}{g} = -\frac{Dg}{g^2}.$$

再利用乘积法则可得除法法则：

$$D\frac{f}{g}=\frac{gDf-fDg}{g^2};$$

$$D(cf)=cDf;$$
$$D(f^n)=nf^{n-1}D(f), \qquad n\in\mathbb{N}.$$

首先给出 $K(X,Y)$ 的所有导数.

命题 2.3.2 对于 $f,g\in K(X,Y)$，在 $K(X,Y)$ 存在唯一的导数 D，使得 $DX=f,DY=g$，对于任意的 $r\in K(X,Y)$，有

$$Dr=\left(\frac{\partial r}{\partial X},\frac{\partial r}{\partial Y}\right)\begin{pmatrix} f\\ g\end{pmatrix}.$$

证明 因为 $K[X,Y]$ 是由 X,Y 生成的 K 代数，且 X,Y 是 K 线性无关的，从导数的定义可知 $K[X,Y]$ 的导数 D 完全由 DX,DY 唯一确定，再利用除法法则可将 D 唯一地扩充为 $K(X,Y)$ 上的导数.

构造如下的 K 线性映射：

$$D':K(X,Y)\to K(X,Y),$$
$$r\mapsto\left(\frac{\partial r}{\partial X},\frac{\partial r}{\partial Y}\right)\begin{pmatrix} f\\ g\end{pmatrix}.$$

易证 D' 是 $K(X,Y)$ 的导数， $D'X=f,D'Y=g$.

因为 E_* 在 $K[X,Y]/(E_*)$ 的分式域 $K(E)$ 中为 0，所以 $K(E)$ 的导数 D 必须满足 $DE_*=D0=0$，即 DX,DY 需要满足特定的关系.

命题 2.3.3 对于 $f\in K(E)$，在 $K(E)$ 上存在唯一导数 D，使得 $DX=f$. 此时，

$$DY=\frac{3X^2+2a_2X+a_4-a_1Y}{2Y+a_1X+a_3}DX.$$

对于任意的 $r\in K(E)$，有

$$Dr=\left(\frac{\partial r}{\partial X},\frac{\partial r}{\partial Y}\right)\begin{pmatrix} DX\\ DY\end{pmatrix}.$$

证明　因为 $DE_* = 0$，即

$$0 = (2Y + a_1X + a_3)DY - (3X^2 + 2a_2X + a_4 - a_1Y)DX,$$

所以 DY 由 DX 唯一确定. 再由命题 2.3.2 知 DX 唯一确定 $K[E]$ 的导数，利用除法法则可将其扩充到 $K(E)$. 该命题中给出的映射 D，满足 $DE_* = 0$，所以 D 是 $K(E)$ 上定义好的. 容易验证 D 是导数.

以上两个命题可以推广到任意函数域：设 L 是 K 上超越次数为 n 函数域，即存在代数无关元 $X_1, \cdots, X_n \in L$，使得 $L/K(X_1, \cdots, X_n)$ 可分，则对于 $f_1, \cdots, f_n \in L$，存在 L 的唯一导数，满足 $DX_i = f_i, 1 \leqslant i \leqslant n$.

有理函数和有理映射复合后的导数值，可由 $K(E)$ 的导数和偏导表示.

命题 2.3.4　设 $\alpha = (\alpha_1, \alpha_2) \in E'(K(E))$ 是有理映射，$r \in K(E')$ 是有理函数，则

$$D(r \circ \alpha) = \left(\frac{\partial r}{\partial X} \circ \alpha, \frac{\partial r}{\partial Y} \circ \alpha\right) \begin{pmatrix} \frac{\partial \alpha_1}{\partial X} & \frac{\partial \alpha_1}{\partial Y} \\ \frac{\partial \alpha_2}{\partial X} & \frac{\partial \alpha_2}{\partial Y} \end{pmatrix} \begin{pmatrix} DX \\ DY \end{pmatrix}.$$

证明　依据复合函数求导法则，可得

$$\frac{\partial r \circ \alpha}{\partial X} = \left(\frac{\partial r}{\partial X} \circ \alpha\right)\left(\frac{\partial \alpha_1}{\partial X}\right) + \left(\frac{\partial r}{\partial Y} \circ \alpha\right)\left(\frac{\partial \alpha_2}{\partial X}\right);$$
$$\frac{\partial r \circ \alpha}{\partial Y} = \left(\frac{\partial r}{\partial X} \circ \alpha\right)\left(\frac{\partial \alpha_1}{\partial Y}\right) + \left(\frac{\partial r}{\partial Y} \circ \alpha\right)\left(\frac{\partial \alpha_2}{\partial Y}\right).$$

再由命题 2.3.3 即得结论.

定义 2.3.5　$K(E)$ 的典型导数 (canonical derivative) 为

$$DX = 2Y + a_1X + a_3 = \frac{\partial E}{\partial Y};$$
$$DY = 3X^2 + 2a_2X + a_4 - a_1Y = -\frac{\partial E}{\partial X};$$
$$Dr = \left(\frac{\partial r}{\partial X}, \frac{\partial r}{\partial Y}\right)\begin{pmatrix} DX \\ DY \end{pmatrix}, \qquad r \in K(E).$$

以下若不作特殊声明，则 D 均指典型导数.

定理 2.3.6 设 m 是正整数，则

$$\begin{aligned}Dg_m &= m(2h_m + a_1 g_m + a_3)\\ &= m\frac{\partial E}{\partial Y}\circ[m],\\ Dh_m &= m(3g_m^2 + 2a_2 g_m + a_4 - a_1 h_m)\\ &= -m\frac{\partial E}{\partial X}\circ[m].\end{aligned}$$

证明 利用数学归纳法证明：

$m=1$ 时，结论显然成立；

$m=2$ 时，有下列关系：

$$\begin{aligned}&DX = 2Y + a_1X + a_3,\ DY = 3X^2 + 2a_2X + a_4 - a_1Y,\\ &\lambda = \frac{3X^2 + 2a_2X + a_4 - a_1Y}{2Y + a_1X + a_3},\\ &g_2 = -2X + \lambda^2 + a_1\lambda - a_2,\\ &h_2 = -(\lambda + a_1)g_2 - a_3 - Y + \lambda X.\end{aligned}$$

则有

$$\begin{aligned}D\lambda = &\frac{((6X + 2a_2)DX - a_1DY)(2Y + a_1X + a_3)}{(2Y + a_1X + a_3)^2}\\ &-\frac{(3X^2 + 2a_2X + a_4 - a_1Y)(2DY + a_1DX)}{(2Y + a_1X + a_3)^2},\\ Dg_2 = &-2DX + 2\lambda D\lambda + a_1D\lambda,\\ Dh_2 = &-(\lambda + a_1)Dg_2 - g_2D\lambda - DY + \lambda DX + XD\lambda.\end{aligned}$$

将 DX, DY 代入，将 Dg_2, Dh_2, g_2, h_2 表示为 X, Y 的有理函数，则得

$$\begin{aligned}Dg_2 &= 2(2h_2 + a_1g_2 + a_3);\\ Dh_2 &= 2(3g_2^2 + 2a_2g_2 + a_4 - a_1h_2).\end{aligned}$$

$m>2$ 时，设对于小于 m 的正整数结论均成立．利用加法公式得

$$\lambda = \frac{h_{m-1} - Y}{g_{m-1} - X},$$

$$\begin{aligned}
g_m &= -g_{m-1} - X + \lambda^2 + a_1\lambda - a_2,\\
h_m &= -(\lambda + a_1)g_m - a_3 - Y + \lambda X,\\
D\lambda &= \frac{(Dh_{m-1} - DY)(g_{m-1} - X)}{(g_{m-1} - X)^2}\\
&\quad -\frac{(h_{m-1} - Y)(Dg_{m-1} - DX)}{(g_{m-1} - X)^2},\\
Dg_m &= -Dg_{m-1} - DX + 2\lambda D\lambda + a_1 D\lambda,\\
Dh_m &= -(\lambda + a_1)Dg_m - g_m D\lambda - DY + \lambda DX + XD\lambda.
\end{aligned}$$

由假设知

$$\begin{aligned}
Dg_{m-1} &= (m-1)(2h_{m-1} + a_1 g_{m-1} + a_3),\\
Dh_{m-1} &= (m-1)(3g_{m-1}^2 + 2a_2 g_{m-1} + a_4 - a_1 h_{m-1}).
\end{aligned}$$

注意到 X, Y 和 g_{m-1}, h_{m-1} 均满足 E 的方程，则将 Dg_{m-1}, Dh_{m-1} 代入可得

$$\begin{aligned}
Dg_m &= m(2h_m + a_1 g_m + a_3),\\
Dh_m &= m(3g_m^2 + 2a_2 g_m + a_4 - a_1 h_m).
\end{aligned}$$

对于多项式 $f \in K[X]$ ，已知 $f' = 0$ 当且仅当存在 $f_1 \in K[X]$, 使得 $f = f_1(X^p)$. 对于有理函数也有类似的结果.

引理 2.3.7 设 $v \in K(X)$ 是单变量有理函数，则

$$v' = 0 \Leftrightarrow \text{存在} v_1 \in K(X), \text{使得} v = v_1(X^p).$$

证明 若 $v = v_1(X^p)$ ，则

$$v' = \frac{\partial v_1(X^p)}{\partial X} = pX^{p-1}v_1'(X^p) = 0.$$

若 $v = 0$ ，结论显然成立. 设 $v = \dfrac{f}{g}, f, g \neq 0 \in K[X]$ ，则

$$0 = v' = \frac{f'g - fg'}{g^2},$$

所以 $f'g = fg'$ ，故 $f|f', g|g'$ ，因为 $\deg\ f' < \deg\ f, \deg\ g' < \deg g$ ，所以

$f' = g' = 0$ ，因此存在 $f_1, g_1 \in K[X]$ ，使得

$$f = f_1(X^p);$$
$$g = g_1(X^p);$$
$$v = \frac{f_1}{g_1}(X^p).$$

定理 2.3.8 设 $r \in K(E), p > 0$ ，则

$$Dr = 0 \Leftrightarrow \text{存在} r_1 \in K(E), \text{使得} r = r_1(X^p, Y^p).$$

证明 若 $r = r_1(X^p, Y^p)$ ，则 $Dr = Dr_1(X^p, Y^p) = 0$. 下证其逆命题成立. 若 $p = 2$ ，则

$$Y^2 = (a_1X + a_3)Y + (X^3 + a_2X^2 + a_4X + a_6), a_1X + a_3 \neq 0,$$

因为 $Y \notin K(X)$, 所以 $Y^2 \notin K(X)$ ；若 $p \neq 2$ ，则 Y^p 是多项式

$$T^2 + a_1^pX^pT + a_3^pT - (X^{3p} + a_2^pX^{2p} + a_4^pX^p + a_6^p) \in K(X)[T]$$

的根，可以证明该多项式在 $K(X)[T]$ 中是不可约的 (同仿射椭圆曲线不可约的证明方法相同)，这说明 $Y^p \notin K(X)$. 综合以上，知 $Y^p \notin K(X)$. 因此 $K(X) \subset K(X, Y^p) \subseteq K(E)$ ，且

$$2 = [K(E) : K(X)] = [K(E) : K(X, Y^p)][K(X, Y^p) : K(X)],$$

故 $K(X, Y^p) = K(E)$ ，即 $\{1, Y^p\}$ 是 $K(E)$ 在 $K(X)$ 上的一组基. 对于 $r \in K(E)$ ，存在 $u, v \in K(X)$ ，使得 $r = u + vY^p$. 则

$$Dr = (u' + v'Y^p)DX + pY^{p-1}vDY = (u' + v'Y^p)DX.$$

$Dr = 0, DX \neq 0$ 可以推出 $u' + v'Y^p = 0$. 因为 $\{1, Y^p\}$ 是基，所以 $u' = v' = 0$. 由引理知存在 $u_1, v_1 \in K(X)$ ，使得 $u = u_1(X^p), v = v_1(X^p)$ ，故

$$r = r_1(X^p, Y^p),$$
$$r_1 = u_1 + Yv_1.$$

对于系数属于特征为 0 的域的多项式 f ，已有结论：若 x 是 f 的 $d > 0$ 阶零点，则 x 是 f' 的 $d-1$ 阶零点. 该结论对于有理函数也成立.

定理 2.3.9 设 r 是有理函数，$P \in E, d = \mathrm{ord}_P(r)$，则有：

(1) 若 $p \nmid d$，则 $\mathrm{ord}_P(Dr) = d - 1$.

(2) 若 $p | d$，则 $\mathrm{ord}_P(Dr) \geqslant d$.

证明 分情况讨论.

(1) 如果 $d = 0$:

①若 $P \neq O$，则 $r = \frac{f}{g}, f, g \in K[E]$，因为 $\mathrm{ord}_P(r) = 0$，所以 $f(P) \neq 0, g(P) \neq 0$，故 $Dr = \dfrac{gDf - fDg}{g^2}$ 在 P 正则，即 $\mathrm{ord}_P(Dr) \geqslant 0$；

②若 $P = O$，则

$$r = u + vY, \qquad u, v \in K(X),$$

$$\mathrm{ord}_O r = \min\{-2\deg u, -3 - 2\deg v\} = 0,$$

所以 $\deg u = 0, -2\deg v \geqslant 4$，若 $u \in K[E]$，则 $u' = 0$；否则，$\deg u' \leqslant -2$. 因为 $\deg v' \leqslant \deg v - 1$，所以 $-2\deg v' \geqslant -2\deg v + 2 \geqslant 6$. 计算得

$$Dr = u'DX + v'YDX + vDY$$

而

$$\mathrm{ord}_O(DX) = \mathrm{ord}_O(2Y + a_1X + a_3) \geqslant -3,$$

$$\mathrm{ord}_O(DY) = \mathrm{ord}_O(3X^2 + 2a_2X + a_4 - a_1Y) \geqslant -4,$$

$$\mathrm{ord}_O(u') = -2\deg u' \geqslant 4$$

$$\mathrm{ord}_O(v') = -2\deg\ v' \geqslant -2(\deg\ v - 1) \geqslant 6.$$

则

$$\mathrm{ord}_O(u'DX) \geqslant 4 - 3 = 1$$

$$\mathrm{ord}_O(v'YDX) \geqslant 6 - 3 - 3 = 0$$

$$\mathrm{ord}_O(vDY) \geqslant 4 - 4 = 0$$

所以 $\mathrm{ord}_O(Dr) \geqslant 0$.

(2) 如果 $d = 1$，则 $r = ut_P$，$u \in K(E), \mathrm{ord}_P(u) = 0, t_P$ 为 P 点的一致性参数. $Dr = t_PDu + uDt_P$. 因为 $\mathrm{ord}_P(u) = 0$，所以由上知

$$\mathrm{ord}_P(t_PDu) = \mathrm{ord}_P(t_P) + \mathrm{ord}_P(Du) \geqslant 1 + 0 = 1.$$

①如果 $P \notin E[2]$，即 $P \neq \overline{P}$，则 $DX = 2Y + a_1X + a_3$ 在 P 点的取值不为 0，所以

$$\begin{aligned} &t_P = X - a; \\ &Dt_P = DX; \\ &\mathrm{ord}_P(Dt_P) = 0; \\ &\mathrm{ord}_P(Dr) = 0. \end{aligned}$$

②如果 $P = (a, b) \in E[2]$，则 $t_P = Y - b, DX|_P = 0, DY|_P \neq 0$，所以

$$\mathrm{ord}_P(Dt_P) = \mathrm{ord}_P(DY) = 0,$$

故 $\mathrm{ord}_P(Dr) = 0$.

③如果 $P = O$，则

$$\begin{aligned} t_O &= \frac{X}{Y}, \\ Dt_O &= \frac{YDX - XDY}{Y^2} = \frac{-X^3 + a_4X + 2a_6 - a_3Y}{X^3 + a_2X^2 + a_4X + a_6 - (a_1X + a_3)Y} \end{aligned},$$

计算得

$$\mathrm{ord}_O(Du) = -6 + 6 = 0,$$

故 $\mathrm{ord}_O(Dr) = 0$.

(3) 如果 $d \geqslant 2$，则 $r = ut_P^d, u \in K(E), \mathrm{ord}_P(u) = 0$，

$$Dr = udt_P^{d-1}Dt_P + t_P^dDu = t_P^{d-1}(udDt_p + t_PDu).$$

若 $p \nmid d$，则有

$$\begin{aligned} &\mathrm{ord}_P(udDt_P) = 0, \\ &\mathrm{ord}_P(t_PDu) \geqslant 1, \end{aligned}$$

所以 $\mathrm{ord}_P(Dr) = d - 1$；如果 $p | d$，则有

$$\mathrm{ord}_P(t_PDu) \geqslant 1,$$

所以 $\mathrm{ord}_P(Dr) \geqslant d$.

(4) 若 $d<0$，则 $\mathrm{ord}_P(r^{-1})=d$， $Dr=-r^2D(r^{-1})$，所以

$$\mathrm{ord}_P(Dr)=2\mathrm{ord}_P(r)+\mathrm{ord}_P(D(r^{-1})).$$

如果 $p|d$，则

$$\mathrm{ord}_P(D(r^{-1}))\geqslant -d,$$
$$\mathrm{ord}_P(Dr)\geqslant d;$$

若 $p\nmid d$，则

$$\mathrm{ord}_P(D(r^{-1}))=-d-1,$$
$$\mathrm{ord}_P(Dr)=d-1.$$

命题 2.3.10 *设 m 是整数，r 是有理函数，则 $D(r\circ[m])=mDr\circ[m]$.*

证明 容易证明满足该命题的所有有理函数组成的集合, 对域运算封闭. 所以只需对 $r=X,Y$, 证明结论成立. 若 $m>0$, 则结论即为定理 2.3.6. 若 $m=-1$, 则有

$$\begin{aligned}D(X\circ[-1])&=DX\\&=2Y+a_1X+a_3\\&=-(2(-Y-a_1X-a_3)+a_1X+a_3)\\&=-DX\circ[-1]\\D(Y\circ[-1])&=D(-Y-a_1X-a_3)\\&=-((3X^2+2a_2X+a_4)-a_1Y)-a_1(2Y+a_1X+a_3)\\&=-((3X^2+2a_2X+a_4)-a_1(-Y-a_1X-a_3))\\&=-DY\circ[-1]\end{aligned}$$

若 $m<-1$，则

$$\begin{aligned}D(r\circ[m])&=D(r\circ[-m]\circ[-1])\\&=-D(r\circ[-m])\circ[-1]\\&=-(-m)Dr\circ[-m]\circ[-1]\\&=mDr\circ[m].\end{aligned}$$

2.4 可 分 性

本节假设 $p>0$.

定义 2.4.1 非零同种 α 称为可分的 (separable)，如果 $e_\alpha=1$；否则，称为不可分.

由推论 2.2.16 可知，α 可分则域扩张 $K(E)/\alpha^*(K(E))$ 是可分的.

命题 2.4.2 对于非零同种 $\alpha\in E'(K(E))$，下列条件等价:

(1) α 不可分;

(2) $D(r\circ\alpha)=0,\ \ \forall r\in K(E')$；

(3) 存在有理函数 $s,t\in K(E)$，使得 $\alpha=(s(X^p,Y^p),t(X^p,Y^p))$.

证明 (1) $\Rightarrow$ (2)：设 α 非可分，存在有理函数 r 使得 $D(r\circ\alpha)\neq 0$. 则 $D(r\circ\alpha)$ 只有有限个零点和极点，所以一定存在点 $P\in E$，满足 $\mathrm{ord}_P D(r\circ\alpha)=0$. 令 $s=r-(r\circ\alpha)(P)$，则 $s\circ\alpha(P)=0$，故 $\mathrm{ord}_P(s\circ\alpha)\geqslant 1$. 另一方面，

$$D(s\circ\alpha)(P)=D(r\circ\alpha)(P)\neq 0,$$

因此 $\mathrm{ord}_P(D(s\circ\alpha))=0$，进而 $\mathrm{ord}_P(s\circ\alpha)=1$. 又因为 $e_\alpha>1$，所以

$$\mathrm{ord}_P(s\circ\alpha)=e_\alpha\mathrm{ord}_{\alpha(P)}(s)>1,$$

矛盾.

(2) $\Rightarrow$ (3)：设 $\alpha=(\alpha_1,\alpha_2)$，分别令 $r=X,Y$，则得

$$D(X\circ\alpha)=D\alpha_1=0,$$
$$D(Y\circ\alpha)=D\alpha_2=0,$$

利用定理 2.3.8 即得结论.

(3) $\Rightarrow$ (1)：已知 $\dfrac{X}{Y}$ 是 O 的一致性参数，则

$$e_\alpha=\mathrm{ord}_O\left(\frac{X}{Y}\circ\alpha\right)=\mathrm{ord}_O\left(\frac{s(X^p,Y^p)}{t(X^p,Y^p)}\right).$$

$$D\left(\frac{X}{Y}\circ\alpha\right)=\frac{t(X^p,Y^p)D(s(X^p,Y^p))-s(X^p,Y^p)D(t(X^p,Y^p))}{t(X^p,Y^p)^2}.$$

由命题 2.3.4 知 $D(s(X^p,Y^p))=0$ ， $D(t(X^p,Y^p))=0$ ，所以 $D\left(\frac{X}{Y}\circ\alpha\right)=0, \mathrm{ord}_O\left(D\left(\frac{X}{Y}\circ\alpha\right)\right)\geqslant 1$ ，利用定理 2.3.9 ，得 $\mathrm{ord}_O\left(\frac{X}{Y}\circ\alpha\right)>1$ ，所以 α 不可分.

推论 2.4.3 设 α,β 是非零同种:

(1) 如果 α,β 不可分，则 $\alpha+\beta$ 也不可分;

(2) 如果 α 可分， β 不可分，则 $\alpha+\beta$ 可分.

命题 2.4.4 设 m 和 p 互素，则 $[m]$ 可分.

证明 设 $P\in E, u$ 是 mP 的一致性参数，则 $e_{[m]}=\mathrm{ord}_P(u\circ[m])$. 由命题 2.3.10 知

$$D(u\circ[m])=mDu\circ[m],$$

所以

$$\begin{aligned}\mathrm{ord}_P(D(u\circ[m]))&=\mathrm{ord}_P(Du\circ[m])\\&=e_{[m]}\mathrm{ord}_{mP}(Du)\\&=0,\end{aligned}$$

则由定理 2.3.9 知 $\mathrm{ord}_P(u\circ[m])=1$ ，即 $[m]$ 可分.

推论 2.4.5 设 $k=\mathbb{F}_q$ ， m,n 是整数且 m 和 p 互素，则 $[m]+[n]\circ\varphi$ 可分.

证明 由推论 2.2.8 和命题 2.2.9 知 $e_{[n]\circ\varphi}=e_{[n]}e_\varphi=qe_{[n]}>1$ ，所以 $[n]\circ\varphi$ 非可分，而已证 $[m]$ 可分，由推论 2.4.3 即得结论.

2.5 $E[m]$ 的群结构

本节的主要目标是研究 $E[m]$ 的群结构， p 均指域 K 的特征. 主要结论为下面两个命题.

命题 2.5.1 若 m 和 p 互素，则 $E[m]\simeq\mathbb{Z}_m\times\mathbb{Z}_m$.

命题 2.5.2 若 $E[p]\neq\{O\}$ ，则 $E[p^v]\simeq\mathbb{Z}_{p^v}$.

结合上述命题，利用群理论，则有如下定理.

定理 2.5.3 设合数 $m=p^vm', p\nmid m'$ ，则:

(1) 若 $E[p]=\{O\}$ ，则 $E[m]\simeq\mathbb{Z}_{m'}\times\mathbb{Z}_{m'}$;

(2) 否则， $E[m] \simeq \mathbb{Z}_{m'} \times \mathbb{Z}_m$.

以上结果均是通过研究 g_m, h_m 和 $g_m - g_n$ 的除子得到的. 为描述方便，引入以下定义.

定义 2.5.4 有理函数 r(在 O) 的首项系数为 $l(r) = \left(\left(\dfrac{X}{Y}\right)^{-\mathrm{ord}_O r} r\right)(O)$.

对于椭圆曲线

$$E : Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6,$$

令 $t = \dfrac{X}{Y}, s = \dfrac{1}{Y}$ ，则得

$$s + a_1ts + a_3s^2 = t^3 + a_2ts + a_4ts^2 + a_6s^3,$$

即

$$\begin{aligned} s &= t^3 + (a_2t - a_1t)s + (a_4t - a_3)s^2 + a_6s^3 \\ &= t^3 + (a_2t - a_1t)t^3 + (a_2t - a_1t)((a_2t - a_1t)s + (a_4t - a_3)s^2 + a_6s^3) \\ &= t^3 + t^4(a_2 - a_1) + \cdots \end{aligned}$$

故

$$\begin{aligned} &Y = \frac{1}{s} = t^{-3}(1 + \cdots), \\ &X = Yt = t^{-2}(1 + \cdots), \\ &l(X) = 1, \\ &l(Y) = 1. \end{aligned}$$

则任意的 $r \in K(E)^\times$ 均可表示为 t 的形式：

$$r = a_dt^d + a_{d+1}t^{d+1} + \cdots ,$$

其中， $a_d \neq 0, d = \mathrm{ord}_O r, l(r) = a_d$. 显然 l 是 $K(E)^\times$ 到 $K^\times$ 的乘性同态. 对于两个在 O 点赋值相同的有理函数 r, s ， $\mathrm{ord}_O(r + s) = \mathrm{ord}_O(r)$ 当且仅当 r, s 的首项系数之和不等于 0. 此时，有 $l(r + s) = l(r) + l(s)$. 注意到 X, Y 的首项系数均为 1 ，所以有理函数乘以 X, Y 的幂次不会改变其首项系数.

命题 2.5.5 设 $p \in \{2, 3\}$ ，则

$$|E[p]| = \begin{cases} p, & \text{若} j \neq 0 \\ 1, & \text{若} j = 0 \end{cases}$$

证明 $p=2$ 时，结论已证明. $p=3$ 时，有限点 $P \in E$ 属于 $E[3]$ 当且仅当 $2P = \pm P$ ，即 $X(2P) = X(P)$ 或 $(g_2 - X)(P) = 0$. 以下依据 E 的正规型分情况证明.

(1) 设 E 的正规型为

$$Y^2 = X^3 + aX^2 + b, \qquad a, b \neq 0$$

此时,

$$\begin{aligned} g_2 &= -2X + \lambda^2 - a, \\ \lambda &= \frac{aX}{Y}. \end{aligned}$$

故

$$\begin{aligned} g_2 - X &= \lambda^2 - a \\ &= \frac{a^2X^2}{Y^2} - a = -\frac{a(X^3+b)}{Y^2}. \end{aligned}$$

可知 $x = -\sqrt[3]{b}$ 是 $g_2 - X = 0$ 的唯一解，所以 $(x, \pm x\sqrt{a})$ 是仅有的两个三阶有限点，即 $|E[3]| = 3$.

(2) 设 E 的正规型为

$$Y^2 = X^3 + aX + b, \qquad a \neq 0$$

此时,

$$g_2 - X = \lambda^2 = \frac{a}{Y^2} \neq 0,$$

故 $g_2 - X$ 无解，即 $E[3] = \{O\}$.

命题 2.5.6 设 $p \in \{2, 3\}$, 定义

$$\alpha = \frac{p^2}{|E[p]|} = \begin{cases} p, & \text{若} j \neq 0 \\ p^2, & \text{若} j = 0 \end{cases}$$

则 $\mathrm{ord}_O g_p = -2\alpha, \mathrm{ord}_O h_p = -3\alpha$. 首项系数为 $l(g_p) = \dfrac{1}{\gamma^2}, l(h_p) = \dfrac{1}{\gamma^3}$ ，其中

$$\gamma = \begin{cases} a_1, & 若 p=2, j\neq 0 \\ a_3, & 若 p=2, j=0 \\ a_1^2+a_2, & 若 p=3, j\neq 0 \\ -(a_1a_3-a_4)^2, & 若 p=3, j=0 \end{cases}$$

证明 分情况讨论如下.

(1) 设 $p=2$ ，则倍点公式为

$$\begin{aligned} \lambda &= \frac{X^2+a_4+a_1Y}{a_1X+a_3}, \\ g_2 &= \lambda^2+a_1\lambda+a_2, \\ h_2 &= \lambda(g_2+X)+Y+(a_1g_2+a_3). \end{aligned}$$

①如果 $j\neq 0$ ，即 $a_1\neq 0$ ，已知 $\mathrm{ord}_O(X)=-2, \mathrm{ord}_O(Y)=-3$ ，所以

$$\begin{aligned} &\mathrm{ord}_O(\lambda)=-2, \\ &l(\lambda)=\frac{1}{a_1}, \\ &\mathrm{ord}_O(g_2)=-4, \\ &l(g_2)=l(\lambda^2)=\frac{1}{a_1^2}, \\ &\mathrm{ord}_O(h_2)=-6, \\ &l(h_2)=l(\lambda)l(g_2)=\frac{1}{a_1^3}. \end{aligned}$$

②如果 $j=0$ ，则 $a_1=0$ ，同上可证结论成立.

(2) 设 $p=3$ ，取椭圆曲线为 $E: Y^2=X^3+a_2X^2+a_4X+a_6$ ，则 $j=0$ 等价于 $a_2=0$. 由倍点公式得

$$\begin{aligned} \lambda_2 &= \frac{-a_2X+a_4}{-Y}, \\ g_2 &= X+\lambda_2^2-a_2, \\ h_2 &= -\lambda_2(g_2-X)-Y. \end{aligned}$$

因为

$$\mathrm{ord}_O(\lambda_2)=\begin{cases} 3, & j=0 \\ 1, & j\neq 0 \end{cases} \qquad l(\lambda_2)=\begin{cases} -a_4, & j=0 \\ a_2, & j\neq 0 \end{cases}$$

所以

$$\begin{aligned}\mathrm{ord}_O(g_2) &= \mathrm{ord}_O X = -2,\\ l(g_2) &= l(X) = 1,\\ \mathrm{ord}_O(h_2) &= \mathrm{ord}_O(-Y) = -3,\\ l(h_2) &= -l(Y) = -1.\end{aligned}$$

再利用加法公式得

$$\begin{aligned}\lambda &= \frac{h_2 - Y}{g_2 - X} = \frac{h_2 - Y}{\lambda_2^2 - a_2},\\ g_3 &= \lambda^2 + (-g_2 - X - a_2),\\ h_3 &= -\lambda g_3 + (\lambda X - Y).\end{aligned}$$

因为 $l(h_2 - Y) = 1$,

$$l(\lambda_2^2 - a_2) = \begin{cases} a_4^2, & j = 0 \\ -a_2, & j \neq 0 \end{cases}$$

结果如表 2.1 所示.

表 2.1 命题 2.5.6 证明数据 (一)

	$j=0$	$j \neq 0$
$\mathrm{ord}_O\lambda$	-9	-3
$l(\lambda)$	$\frac{1}{a_4^2}$	$-\frac{1}{a_2}$
$\mathrm{ord}_O(g_3)$	-18	-6
$l(g_3)$	$\frac{1}{a_4^4}$	$\frac{1}{a_2^2}$
$\mathrm{ord}_O(h_3)$	-27	-9
$l(h_3)$	$-\frac{1}{a_4^6}$	$\frac{1}{a_2^3}$

又因为椭圆曲线 $E': Y^2 + a_1XY + a_3Y = X^3 + a_2X^2 + a_4X + a_6$ 同构于椭圆曲线 $Y^2 = X^3 + b_2X^2 + b_4X + b_6$，其中

$$\begin{aligned}b_2 &= a_1^2 + a_2,\\ b_4 &= a_1a_3 - a_4,\\ b_6 &= a_3^2 + a_6,\end{aligned}$$

故对于 E' 有如表 2.2 所示表格.

结论得证.

命题 2.5.7 设 m 是与 p 互素的正整数，则

$$\operatorname{ord}_O(g_m) = -2, \qquad \operatorname{ord}_O(h_m) = -3,$$
$$l(g_m) = \frac{1}{m^2}, \qquad l(h_m) = \frac{1}{m^3}.$$

表 2.2 命题 2.5.6 证明数据 (二)

	$j=0$	$j\neq 0$
$\operatorname{ord}_O(g_3)$	-18	-6
$l(g_3)$	$\dfrac{1}{(a_1a_3-a_4)^4}$	$\dfrac{1}{(a_1^2+a_2)^2}$
$\operatorname{ord}_O(h_3)$	-27	-9
$l(h_3)$	$-\dfrac{1}{(a_1a_3-a_4)^6}$	$\dfrac{1}{(a_1^2+a_2)^3}$

证明 利用数学归纳法证明. 注意对于 p 的幂次，结论不再成立，故若 m 为 p 的幂次时，这里的递归步将直接由 $m-1$ 到 $m+1$. 首先假设 $p\neq 2,3$ ，椭圆曲线为正规型 $Y^2=X^3+a_4X+a_6$. 需要强调的是：有理函数的首项系数均是属于 $\mathbb{F}_q$ 的.

(1) 若 $m=1$, 则 $g_1=X, h_1=Y$ ，结论显然成立.

(2) 若 $m=2$ ，倍点公式为

$$\lambda = \frac{3X^2+a_4}{2Y},$$
$$g_2 = -2X+\lambda^2,$$
$$h_2 = -\lambda(g_2-X)-Y,$$

则 $\operatorname{ord}_O\lambda=-1, l(\lambda)=\dfrac{3}{2}, \operatorname{ord}_O(-2X)=-2, \operatorname{ord}_O(\lambda^2)=-2$, 而 $l(-2X)+l(\lambda^2)=\dfrac{1}{4}$ ，故

$$\operatorname{ord}_O g_2=-2, \qquad l(g_2)=\frac{1}{4}.$$

又因为

$$\begin{aligned} l(-\lambda(g_2-X))-l(Y) &= \frac{3}{2}\left(1-\frac{1}{4}\right)-1 \\ &= \frac{1}{8}, \end{aligned}$$

所以

$$\text{ord}_O h_2 = -3, \qquad l(h_2) = \frac{1}{8}.$$

(3) 若 $m \not\equiv 0,1,2(\text{mod } p)$，现假设对于 $m-1$ 结论成立，证明对于 m 结论也成立. 由加法公式得

$$\lambda = \frac{h_{m-1} - Y}{g_{m-1} - X},$$
$$g_m = -g_{m-1} - X + \lambda^2,$$
$$h_m = -\lambda(g_m - X) - Y.$$

因为

$$\begin{aligned}
& l(g_{m-1}) - l(X) = 0 \\
\Leftrightarrow & \frac{1}{(m-1)^2} - 1 \equiv 0(\text{mod} p) \\
\Leftrightarrow & (m-1)^2 \equiv 1(\text{mod} p) \\
\Leftrightarrow & m - 1 \equiv \pm 1(\text{mod} p) \\
\Leftrightarrow & m \equiv 0, 2(\text{mod} p),
\end{aligned}$$

所以 $l(g_{m-1}) - l(X) \neq 0$， $\text{ord}_O(g_{m-1} - X) = -2$.

①如果 $(m-1)^3 \not\equiv 1(\text{mod } p)$，则类似 $l(g_{m-1}) - l(X)$ 的分析可知 $l(h_{m-1}) - l(Y) \neq 0$，利用归纳假设知 $\text{ord}_O\lambda = -1$,

$$l(\lambda) = \frac{l(h_{m-1}) - l(Y)}{l(g_{m-1}) - l(X)} = \frac{\dfrac{1}{(m-1)^3} - 1}{\dfrac{1}{(m-1)^2} - 1} = \frac{m^2 - m + 1}{m(m-1)}.$$

故 g_m 的各项在 O 的赋值均为 -2，且首项系数之和

$$\begin{aligned}
& -l(g_{m-1}) - l(X) + l(\lambda)^2 \\
= & -\frac{1}{(m-1)^2} - 1 + \left(\frac{m^2 - m + 1}{m(m-1)}\right)^2 \\
= & \frac{1}{m^2} \neq 0.
\end{aligned}$$

则得 $\text{ord}_O g_m = -2, l(g_m) = \dfrac{1}{m^2}$，对 h_m 可以类似计算得

$$-l(\lambda)(l(g_m) - l(X)) - l(Y)$$

$$
\begin{aligned}
&= -\frac{m^2-m+1}{m(m-1)} \cdot \frac{1-m^2}{m^2} - 1 \\
&= \frac{1}{m^3} \neq 0,
\end{aligned}
$$

故 $\mathrm{ord}_O h_m = -3, l(h_m) = \dfrac{1}{m^3}$.

②如果 $(m-1)^3 \equiv 1 (\bmod\ p)$，则 $l(h_{m-1}) = l(Y) = 1$，因此 $\mathrm{ord}_O(h_{m-1} - Y) \geqslant -2$，所以 λ 在 O 点正则. 在 g_m 的表达式中仅 $-g_{m-1} - X$ 在 O 点非正则，而

$$
l(-g_{m-1} - X) = -\frac{1}{(m-1)^2} - 1 = -(m-1) - 1 = -m = \frac{-m^3}{m^2} \neq 0,
$$

所以 $\mathrm{ord}_O g_m = -2$. 又因为 $m \not\equiv 2 (\bmod p)$，所以 $m+1 \not\equiv 0 (\bmod p)$，且由

$$
\begin{aligned}
0 &= (m-1)^3 - 1 \\
&= m^3 - 3m^2 + 3m - 2 \\
&= (m^3+1)\left(1 - \frac{3}{m+1}\right)
\end{aligned}
$$

可知在 $\mathbb{F}_p$ 中有 $-m^3 = 1$，所以

$$
\begin{aligned}
l(-g_{m-1} - X) &= \frac{1}{m^2}, \\
l(g_m) &= \frac{1}{m^2}.
\end{aligned}
$$

分析 h_m 的表达式，可知

$$
\begin{aligned}
\mathrm{ord}_O h_m &= \mathrm{ord}_O(-Y) = -3, \\
l(h_m) &= l(-Y) = -1 = \frac{1}{m^3}.
\end{aligned}
$$

(4) 若 $m \equiv 1 (\bmod\ p)$，归纳假设对于 $m-2$ 结论均成立，则证明结论对于 m 也成立. 因为 $p \neq 3$, 所以 $m \neq 4$，则由 $[m-2], [2]$ 利用加法公式可得

$$
\begin{aligned}
\lambda &= \frac{h_{m-2} - h_2}{g_{m-2} - g_2}, \\
g_m &= -g_{m-2} - g_2 + \lambda^2, \\
h_m &= -\lambda(g_m - g_2) - h_2.
\end{aligned}
$$

注意到 $m-2 \equiv -1(\mathrm{mod}\ p)$，同上计算可得 $\mathrm{ord}_O\lambda = -1, \mathrm{ord}_O g_m = -2, \mathrm{ord}_O h_m = -3$,

$$\begin{aligned}
l(\lambda) &= \frac{l(h_{m-2}) - l(h_2)}{l(g_{m-2}) - l(g_2)} = \frac{\dfrac{1}{(m-2)^3} - \dfrac{1}{8}}{\dfrac{1}{(m-2)^2} - \dfrac{1}{4}} \\
&= \frac{\dfrac{1}{(-1)^3} - \dfrac{1}{8}}{\dfrac{1}{(-1)^2} - \dfrac{1}{4}} = -\frac{3}{2} \neq 0, \\
l(g_m) &= -l(g_{m-2}) - l(g_2) + l(\lambda)^2 \\
&= -\frac{1}{(-1)^2} - \frac{1}{4} + \frac{9}{4} = 1 = \frac{1}{m^2}, \\
l(h_m) &= -l(\lambda)(l(g_m) - l(g_2)) - l(h_2) \\
&= \frac{3}{2}(1 - \frac{1}{4}) - \frac{1}{8} = 1 = \frac{1}{m^3}.
\end{aligned}$$

(5) 若 $m \equiv 2(\mathrm{mod}\ p)$，归纳假设结论对于 $m-3$ 成立，则证明对于 m 结论也成立．显然 $m=6$ 不属于该情况．所以可以利用加法公式由 $[m-3],[3]$ 计算得

$$\lambda = \frac{h_{m-3} - h_3}{g_{m-3} - g_3},$$

$$g_m = -g_{m-3} - g_3 + \lambda^2,$$

$$h_m = -\lambda(g_m - g_3) - h_3.$$

注意：$m-3 \equiv -1(\mathrm{mod}\ p)$．因为 $l(g_{m-3} - g_3) = \dfrac{1}{(m-3)^2} - \dfrac{1}{9} = 1 - \dfrac{1}{9} = \dfrac{8}{9} \neq 0$，所以 $\mathrm{ord}_O(g_{m-3} - g_3) = -2$．已知 $l(h_{m-3}) = -1, l(h_3) = \dfrac{1}{27}$，则分情况计算 g_m, h_m 在 O 的赋值、首项系数．

①如果 $p \neq 7$，则 $l(h_{m-3}) \neq l(h_3)$，所以 $\mathrm{ord}_O\lambda = -1$，$l(\lambda) = \dfrac{-1 - \dfrac{1}{27}}{1 - \dfrac{1}{9}} = -\dfrac{7}{6}$．同上计算可得 $\mathrm{ord}_O g_m = -2, \mathrm{ord}_O h_m = -3$,

$$l(g_m) = -l(g_{m-3}) - l(g_3) + l(\lambda)^2$$

$$
\begin{aligned}
&= -1 - \frac{1}{9} + \frac{49}{36} = \frac{1}{4} = \frac{1}{m^2}, \\
l(h_m) &= -l(\lambda)(l(g_m) - l(g_3)) - l(h_3) \\
&= \frac{7}{6}(\frac{1}{4} - \frac{1}{9}) - \frac{1}{27} = \frac{1}{8} = \frac{1}{m^3}.
\end{aligned}
$$

②如果 $p = 7$ ，则 $l(h_{m-3}) - l(h_3) = 0$ ，所以 λ 在 O 点正则，同上计算得 $\mathrm{ord}_O g_m = -2, \mathrm{ord}_O h_m = -3$,

$$
\begin{aligned}
l(g_m) &= -l(g_{m-3}) - l(g_3) \\
&= -1 - \frac{1}{9} = -\frac{10}{9} = \frac{1}{4} = \frac{1}{m^2}, \\
l(h_m) \quad &= -l(h_3) = -\frac{1}{27} = \frac{1}{8} = \frac{1}{m^3}.
\end{aligned}
$$

以上证明了对于 $p \notin \{2,3\}$ ， $E: Y^2 = X^3 + a_4 X + a_6$ 结论成立. 因为定义在特征为 p 的有限域上的任意椭圆曲线 $Y^2 + a_1 XY + a_3 = X^3 + a_2 X^2 + a_4 X + a_6$ 均同构于椭圆曲线 $Y^2 = X^3 + b_4 X + b_6$ ，所以结论对于 $p \notin \{2,3\}$ 上的椭圆曲线均成立.

以下假设 $p \in \{2,3\}$.$m = 1$ 时，结论显然成立. 当 $m = 2$ 时， p 只能为 3 ，结论的正确性从命题 2.5.6 的证明过程可知. 已知 $m \not\equiv 0 \mod p$ ，假设结论对于 $m - p$ 成立，则证明对于 m 结论也成立. α, γ 的定义同命题 2.5.6. 由 $[m-p], [p]$ 得

$$
\begin{aligned}
\lambda &= \frac{h_p - h_{m-p}}{g_p - g_{m-p}}, \\
g_m &= -g_{m-p} - g_p + \lambda^2 + a_1 \lambda - a_2, \\
h_m &= -\lambda(g_m - g_p) - h_p - (a_1 g_m + a_3).
\end{aligned}
$$

由命题 2.5.6 知 $\mathrm{ord}_O(\lambda^2) = \mathrm{ord}_O g_p = -2\alpha$. 以下计算 $\mathrm{ord}_O(g_m - g_{m-p}), l(g_m - g_{m-p})$.

$$
g_m - g_{m-p} = -2g_{m-p} - g_p + \lambda^2 + a_1\lambda - a_2 = \frac{r}{s},
$$

其中

$$
\begin{aligned}
s &= g_p^2 - 2g_p g_{m-p} + g_{m-p}^2, \\
r &= -(g_p^2 - 2g_p g_{m-p} + g_{m-p}^2)(g_p + 2g_{m-p} + a_2)
\end{aligned}
$$

$$
\begin{aligned}
&+(h_p^2-2h_ph_{m-p}+h_{m-p}^2)+a_1(h_p-h_{m-p})(g_p-g_{m-p})\\
=&(h_p^2+a_1h_pg_p-g_p^3-a_2g_p^2)\\
&+(h_{m-p}^2+a_1h_{m-p}g_{m-p}-2g_{m-p}^3-a_2g_{m-p}^2)\\
&+3g_pg_{m-p}^2+2a_2g_pg_{m-p}-2h_ph_{m-p}-a_1h_pg_{m-p}-a_1h_{m-p}g_p\\
=&-a_3h_p+a_4g_p-a_3h_{m-p}-g_{m-p}^3+a_4g_{m-p}+2a_6\\
&+3g_pg_{m-p}^2+2a_2g_pg_{m-p}-2h_ph_{m-p}-a_1h_pg_{m-p}-a_1h_{m-p}g_p.
\end{aligned}
$$

再利用命题 2.5.6 和归纳假设即得 $\mathrm{ord}_O s=-4\alpha, l(s)=\dfrac{1}{\gamma^4}$. $p=3$ 时，r 中阶最小的项为 $-2h_ph_{m-p}=h_ph_{m-p}$，所以 $\mathrm{ord}_O r=-3\alpha-3, l(r)=\dfrac{1}{\gamma^3(m-p)^3}=\dfrac{1}{\gamma^3m^3}$. $p=2$ 时，r 中 $a_1h_pg_{m-p}$ 的阶最小，故 $\mathrm{ord}_O r\geqslant -3\alpha-2$. 总结以上，有结论

$$
\begin{aligned}
&\mathrm{ord}_O(g_m-g_{m-p})=\alpha-3, && p=3;\\
&l(g_m-g_{m-p})=\frac{\gamma}{m^3}, && p=3;\\
&\mathrm{ord}_O(g_m-g_{m-p})\geqslant\alpha-2, && p=2.
\end{aligned}
$$

因为 $\alpha\geqslant p$，所以 $\mathrm{ord}_O(g_m-g_{m-p})\geqslant 0$，而 $\mathrm{ord}_O g_{m-p}=-2$，故

$$
\begin{aligned}
&\mathrm{ord}_O g_m=\mathrm{ord}_O g_{m-p}=-2,\\
&l(g_m)=l(g_{m-p})=\frac{1}{(m-p)^2}=\frac{1}{m^2}.
\end{aligned}
$$

合并 h_m 中阶至多为 -3 的项得

$$
\begin{aligned}
-\lambda(g_m-g_p)-h_p&=\frac{-(h_p-h_{m-p})(g_m-g_p)-h_p(g_p-g_{m-p})}{g_p-g_{m-p}}\\
&=\frac{-h_p(g_m-g_{m-p})-h_{m-p}g_p+h_{m-p}g_m}{g_p-g_{m-p}},
\end{aligned}
$$

分母在 O 点的阶为 -2α，首项系数为 $\dfrac{1}{\gamma^2}$. 若 $p=3$, 则

$$
\begin{aligned}
&\mathrm{ord}_O(h_p(g_{m-p}-g_m))=-2\alpha-3,\\
&\mathrm{ord}_O(h_{m-p}g_m)=-5,\\
&\mathrm{ord}_O(h_{m-p}g_p)=-2\alpha-3,
\end{aligned}
$$

且

$$l(-h_p(g_m-g_{m-p}))+l(-h_{m-p}g_p)=-\frac{1}{\gamma^3}\cdot\frac{\gamma}{m^3}-\frac{1}{m^3}\cdot\frac{1}{\gamma^2}=\frac{1}{\gamma^2m^3}.$$

由此知分子在 O 点的阶为 $-2\alpha-3$，首项系数为 $\dfrac{1}{\gamma^2m^3}$，所以 $p=3$ 时，

$$\begin{aligned}&\mathrm{ord}_O(-\lambda(g_m-g_p)-h_p)=-3,\\&l(-\lambda(g_m-g_p)-h_p)=\frac{1}{m^3},\\&\mathrm{ord}_O(h_m)=-3,\\&l(h_m)=\frac{1}{m^3}.\end{aligned}$$

若 $p=2$，则 $\mathrm{ord}_O(h_p(g_{m-p}-g_m))\geqslant-2\alpha-2$，所以

$$\begin{aligned}&\mathrm{ord}_O(-\lambda(g_m-g_p)-h_p)=-3,\\&l(-\lambda(g_m-g_p)-h_p)=-\frac{1}{\gamma^2m^3},\\&\mathrm{ord}_Oh_m=-3,\\&l(h_m)=\frac{1}{m^3}.\end{aligned}$$

命题 2.5.8　设 $p\in\{2,3\}$，整数$m=p^vm'$，m' 和 p 互素，则

$$\begin{aligned}&\mathrm{ord}_Og_m=-2\alpha^v,\\&\mathrm{ord}_Oh_m=-3\alpha^v,\\&e_{[m]}=\alpha^v,\end{aligned}$$

其中 α 的定义见命题 2.5.6.

证明　$v=0$ 时，结论即为命题 2.5.7 、命题 2.4.4.

假设对于 $m=p^vm'$ 结论成立，证明对于 pm 结论也成立.

$$\begin{aligned}\mathrm{ord}_Og_{pm}&=\mathrm{ord}_O(g_p\circ[m])\\&=e_{[m]}\mathrm{ord}_Og_p\\&=\alpha^v(-2\alpha)\\&=-2\alpha^{v+1}.\end{aligned}$$

同理可以求得 $\mathrm{ord}_Oh_{pm}=-3\alpha^{v+1}$. 已知 $\dfrac{X}{Y}$ 是 O 的一致性参数，则

$$e_{[pm]}=\mathrm{ord}_O\left(\frac{X}{Y}\circ[pm]\right)=\mathrm{ord}_O\left(\frac{g_{pm}}{h_{pm}}\right)=\alpha^{v+1}.$$

对于 $p=2$，其首项系数见表 2.3(读者可以作为练习 (见习题 2.5) 给出证明).

表 2.3　首项系数

$j \neq 0$	$j = 0$	
$l(g_m)$	$\frac{1}{a_1^{2(2^v-1)}}$	$\frac{1}{a_3^{\frac{2}{3}(4^v-1)}}$
$l(h_m)$	$\frac{1}{a_1^{3(2^v-1)}}$	$\frac{1}{a_3^{4^v-1}}$

接下来研究 g_m-g_n 所决定的除子. 令 $<E[m]>$ 表示 $E[m]$ 中点的系数为 1，其余点的系数为 0 的除子.

命题 2.5.9　设 m,n 是非零整数:

(1) 如果 $p\neq 2,3$ 且 $m,n,m+n,m-n$ 均和 p 互素，则

$$\operatorname{div}(g_m-g_n)=<E[m+n]>+<E[m-n]>-2<E[m]>-2<E[n]>.$$

(2) 如果 $p\in\{2,3\}, m$ 和 p 互素，$n=p^v n', v\geqslant 1, n'$ 和 p 互素，则 $\operatorname{div}(g_m-g_n)=<E[m+n]>+<E[m-n]>-2<E[m]>-2\alpha^v<E[n]>$. 其中 α 的定义见命题 2.5.6.

证明　仅给出 $p\in\{2,3\}$ 的证明, 其他的情况请读者作为练习 (见习题 2.7)，证明方法是类似的. 注意 $g_m(g_n)$ 的极点一定属于 $E[m](E[n])$，所以 g_m-g_n 的极点一定属于 $E[m]\cup E[n]$. 若 $(g_m-g_n)(P)=0$，则 $X(mP)=X(nP)$，等价于 $mP=\pm nP$，所以 g_m-g_n 的零点一定属于 $E[m+n]\cup E[m-n]$. 故 g_m-g_n 仅在 $m,n,(m+n),(m-n)$ 扭点的赋值可能不为 0. 设 $P\in E[m]\cup E[n]\cup E[m+n]\cup E[m-n]$：

(1) 若 $P=O$，由命题 2.5.7、命题 2.5.8 知 $\operatorname{ord}_O g_m=-2, \operatorname{ord}_O g_n=-2\alpha^v<-2$，所以 $\operatorname{ord}_O(g_m-g_n)=-2\alpha^v$.

(2) 若 $P\in(E[m]\cap E[n])\setminus\{O\}$，则 $P\in E[m+n]\cap E[m-n]$. 因为 g_m, g_n 在 $E[m]\cap E[n]$ 中点的移位作用下保持不动，所以有

$$\begin{aligned}\operatorname{ord}_P(g_m-g_n)&=\operatorname{ord}_P((g_m-g_n)\circ\tau_{-P})\\&=e_{\tau_{-P}}(P)\operatorname{ord}_{\tau_{-P}(P)}(g_m-g_n)\\&=\operatorname{ord}_O(g_m-g_n).\end{aligned}$$

(3) 若 $P \in E[m] \setminus E[n]$，则 $P \notin E[m+n] \cup E[m-n]$. 因为 g_m 在 P 移位作用下保持不动，所以同上可得 $\mathrm{ord}_P g_m = \mathrm{ord}_O g_m = -2$. 而 g_n 在 $P \notin E[n]$ 正则，故 $\mathrm{ord}_P(g_m - g_n) = -2$.

(4) 若 $P \in E[n] \setminus E[m]$，由命题 2.5.8 知 $\mathrm{ord}_P g_n = \mathrm{ord}_O g_n = -2\alpha^v$，而 $P \notin E[m]$ 说明 $\mathrm{ord}_P g_m \geqslant 0$，所以 $\mathrm{ord}_P(g_m - g_n) = -2\alpha^v$.

以下均假设 $P \notin E[m] \cup E[n]$.

(5) 若 $P \in E[m-n] \setminus E[m+n]$，即 $mP = nP \neq -nP$. 显然 $(g_m - g_n)(P) = 0$. 因为

$$
\begin{aligned}
D(g_m - g_n) &= m(2h_m + a_1 g_m + a_3) - n(2h_n + a_1 g_n + a_3) \quad (\text{由定理 } 2.3.6) \\
&= m(2h_m + a_1 g_m + a_3)
\end{aligned}
$$

因为 $p|n$, 所以

$$
\begin{aligned}
D(g_m - g_n)(P) &= m(2h_m(P) + a_1 g_m(P) + a_3) \\
&= m(2Y + a_1 X + a_3)(mP) \\
&\neq 0
\end{aligned}
$$

若 $(2Y + a_1 X + a_3)(mP) = 0$，因为 $mP \neq O$，所以 $mP = -mP$，矛盾. 由上得 $\mathrm{ord}_P(D(g_m - g_n)) = 0$，再利用定理 2.3.9 得 $\mathrm{ord}_P(g_m - g_n) = 1$.

(6) 若 $P \in E[m+n] \setminus E[m-n]$，即 $mP = -nP \neq nP$，同上分析可知 $\mathrm{ord}_P(g_m - g_n) = 1$.

(7) 若 $P \in E[m+n] \cap E[m-n]$，即 $mP = nP$ 是 2 阶点. 显然 $(g_m - g_n)(P) = 0$. 按域特征分情况讨论.

①设 $p = 3$. 因为 $D(g_m - g_n) = m(-h_m + a_1 g_m + a_3)$， mP 是 2 阶点, 所以 $D(g_m - g_n)(P) = 0$. 由定理 2.3.4 知 $D^2(g_m - h_m) = m^2(a_2 g_m - a_4 + a_1 h_m + a_1(-h_m + a_1 g_m + a_3))$，所以

$$
\begin{aligned}
D^2(g_m - g_n)(P) &= m^2(a_2 g_m - a_4 + a_1 h_m)(P) \\
&= m^2 \frac{\partial E}{\partial X}(mP) \\
&\neq 0 \quad \text{因为} \frac{\partial E}{\partial Y}(mP) = 0
\end{aligned}
$$

再利用定理 2.3.9 知 $\mathrm{ord}_P(g_m - g_n) = 2$.

②设 $p=2$. 无法利用定理 2.3.9 求得 $\mathrm{ord}_P(g_m-g_n)$，可以通过求 $\mathrm{ord}_P(a_1g_m+a_3)$, $\mathrm{ord}_P(a_1g_n+a_3)$ 来获得 $\mathrm{ord}_P(g_m-g_n)$. 因为 mP 是 2 阶点，所以 $a_1\neq 0$.

$$\begin{aligned}\mathrm{ord}_P(a_1g_m+a_3)&=\mathrm{ord}_P((a_1X+a_3)\circ[m])\\&=e_{[m]}\mathrm{ord}_{mP}(a_1X+a_3).\end{aligned}$$

由命题 2.4.4 知 $e_{[m]}=1$，而 mP 是 2 阶点，所以 $\mathrm{ord}_{mP}(a_1X+a_3)=2$, $\mathrm{ord}_P(a_1g_m+a_3)=2$.

$$\begin{aligned}\mathrm{ord}_P(a_1g_n+a_3)&=e_{[n]}\mathrm{ord}_{nP}(a_1X+a_3)\\&=\alpha^v\cdot 2\\&>2,\end{aligned}$$

所以 $\mathrm{ord}_P(g_m-g_n)=\mathrm{ord}_P((a_1g_m+a_3)-(a_1g_n+a_3))=2$.

命题 2.5.10　*设整数 m 和 p 互素，则 $|E[m]|=m^2$.*

证明　令 $d_{m'}$ 表示 $|E[m']|$. 假设 $p\neq 2,3$. 因为主除子的次数为 0，所以由命题 2.5.9 知若 $m',n',m'+n',m'-n'$ 和 p 互素，有

$$d_{m'+n'}+d_{m'-n'}-2d_{m'}-2d_{n'}=0.$$

以下用数学归纳法证明结论成立. $m=1,2$ 时，结论显然成立. 设对于 $r<m, p\nmid r$ 有 $d_r=r^2$.

(1) 若 $m\not\equiv 1,2 \mod p$. 令 $n'=1, m'=m-1$，则

$$\begin{aligned}d_m&=2d_{m-1}+2d_1-d_{m-2}\\&=2(m-1)^2+2-(m-2)^2=m^2.\end{aligned}$$

(2) 若 $m\equiv 1 \mod p, m\geqslant p+1$. 因为 $p\neq 2,3$，所以 $p\geqslant 5, m\not\equiv 2,4 \mod p$. 令 $n'=2, m'=m-2$，则有

$$\begin{aligned}d_m&=2d_{m-2}+2d_2-d_{m-4}\\&=2(m-2)^2+8-(m-4)^2=m^2.\end{aligned}$$

(3) 若 $m\equiv 2 \mod p, m\geqslant p+2$. 因为 $p\geqslant 5$，所以 $m\not\equiv 3,6 \mod p$. 令 $n'=3, m'=m-3$，则有

$$\begin{aligned}d_m&=2d_{m-3}+2d_3-d_{m-6}\\&=2(m-3)^2+18-(m-6)^2=m^2.\end{aligned}$$

假设 $p=2,3,m$ 和 p 互素. $d_1=d_{-1}=1$. 对于 $p=3$，有 $d_2=d_{-2}=4$. 设对于小于 m 且与 p 互素的整数结论均成立, 证明对于 m 结论也成立. 令 $n=p$，利用命题 2.5.9 可得

$$d_m=2d_{m-p}+2\alpha d_p-d_{m-2p},$$

由 α 的定义知 $\alpha d_p=p^2$，因此

$$\begin{aligned}d_m&=2(m-p)^2+2p^2-(m-2p)^2\\&=m^2.\end{aligned}$$

定理 2.5.11 (有限 Abelian 群基本定理) *设有限 Abelian 群 $G\neq\{0\}$，则存在唯一的正整数 r 和 $n_1,\cdots,n_r\geqslant 2$, 使得 $n_i|n_{i+1},i=1,\cdots,r-1$，且*

$$G\simeq\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_r}.$$

命题 2.5.1 的证明 对 m 的素因子个数进行递归来证明结论:

(1) 设 $m=q$ 是素数, 则利用定理 2.5.11 知 $E[q]\simeq\mathbb{Z}_q\times\mathbb{Z}_q$ 或 $E[q]\simeq\mathbb{Z}_{q^2}$ 是循环群. 若 $E[q]$ 是循环群, 则 $E[q]$ 中存在 q^2 阶点, 矛盾.

(2) 设对于 m' 结论成立, 证明对于 $m=qm',|m'|>1,q$ 是素数, $E[m]\simeq\mathbb{Z}_{n_1}\times\cdots\times\mathbb{Z}_{n_r}$. 因为 $[q]$ 是满射, 所以

$$\begin{aligned}E[m']&=\{P:m'P=O\}\\&=\{qP:m'qP=O\}\\&=\{qP:P\in E[m]\}\\&=qE[m],\end{aligned}$$

则

$$\begin{aligned}E[m']&\simeq q\mathbb{Z}_{n_1}\times\cdots\times q\mathbb{Z}_{n_r}\\&\simeq\mathbb{Z}_{b_1}\times\cdots\times\mathbb{Z}_{b_r},\end{aligned}$$

其中

$$b_i=\begin{cases}n_i, & q\nmid n_i\\ \dfrac{n_i}{q}, & q|n_i\end{cases}$$

因为 $n_i|n_{i+1}$ ，所以 $b_i|b_{i+1}$. 由假设知 $b_1 = \cdots = b_{r-2} = 1, b_{r-1} = b_r = m'$ ，故 $n_1 = \cdots = n_{r-2} = q, n_{r-1} = n_r = qm' = m$. 而 $|E[m]| = m^2 = q^{r-2}m^2$ ，所以 $r = 2$.

引理 2.5.12 *p 扭点的个数小于 p^2.*

证明 $p = 2, 3$ 的结论已证明. 对于任意的特征，在下节将利用可除多项式 (division polynomial) 证明.

命题 2.5.2 的证明 由引理得 $E[p] = \{O\}$ 或 $E[p] \simeq \mathbb{Z}_p$ ，再利用已知条件得 $E[p] \simeq \mathbb{Z}_p$. 对 v 做归纳：假设 $E[p^{v-1}] \simeq \mathbb{Z}_{p^{v-1}}$ ，证明对于 p^v 结论也成立. 考虑群同态：

$$\rho : E[p^v] \to E[p^{v-1}],$$
$$P \mapsto pP,$$

因为 $[p]$ 是满射，p^{v-1} 扭点对于 $[p]$ 的原像一定是 p^v 扭点，所以 ρ 也是满的，其核为 $E[p]$ ，故 $|E[p^v]| = |\mathrm{im}\rho||\ker\rho| = p^{v-1}p = p^v$. 由归纳假设知，存在 p^{v-1} 阶点，设为 Q ，则 Q 相对于 ρ 的任意原像均是 p^v 阶点，所以 $E[p^v]$ 是循环群.

引理 2.5.13 *若整数 m, n 互素，则 $E[mn] \simeq E[m] \times E[n]$.*

证明 因为 m, n 互素，所以存在整数 a, b, 使得 $am + bn = 1$. 定义如下群同态：

$$\iota : E[m] \times E[n] \to E[mn],$$
$$(P, Q) \mapsto P + Q,$$
$$\pi : E[mn] \to E[m] \times E[n],$$
$$P \mapsto (bnP, amP).$$

容易验证 ι, π 是定义好的群同态. 下证 $\pi \circ \iota = id|_{E[m]\times E[n]}, \iota \circ \pi = id|_{E[mn]}$:

$$\begin{aligned}
\pi \circ \iota(P, Q) &= (bn(P + Q), am(P + Q)) \\
&= (bnP, amQ) \\
&= ((bn + am)P, (bn + am)Q) \\
&= (P, Q), \\
\iota \circ \pi(P) &= (bn + am)P = P,
\end{aligned}$$

所以 $E[mn] \simeq E[m] \times E[n]$.

定理 2.5.3 的证明 对于 $m = p^v m', p \nmid m'$，由引理得

$$E[m] \simeq E[m'] \times E[p^v].$$

如果 $E[p] = \{O\}$，则 $E[p^v] = \{O\}$，

$$E[m] \simeq E[m'] \simeq \mathbb{Z}_{m'} \times \mathbb{Z}_{m'}.$$

否则,

$$E[m] \simeq \mathbb{Z}_{m'} \times \mathbb{Z}_{m'} \times \mathbb{Z}_{p^v} \simeq \mathbb{Z}_{m'} \times \mathbb{Z}_{m}.$$

2.6 可除多项式

上节已说明 g_m, h_m 的极点恰好是 m 扭点，那么是否存在有理函数，使得其零点恰好是所有的 m 扭点且阶均为 1，极点仅有 O. 若该有理函数存在，因为其没有有限极点，所以它一定是多项式. 又由 E 同构于 $\mathrm{Pic}^0(E)$ 可得，该多项式存在，当且仅当 m 扭点的和为 O. 对于和 p 互素的整数 m 该结论是成立的：若 P 是 m 扭点，则 $\overline{P}$ 也是 m 扭点. 所以非 2 阶点的所有 m 扭点的和为 O. 若 $E[m]$ 中有 2 阶点，则 m 一定为偶数，若 $p \neq 2$，则存在三个 2 阶点，因为 $E[2] \subseteq E[m]$， $\mathrm{div}(2Y + a_1X + a_3) =< E[2] > -4 < O >$，所以所有 2 阶点的和为 O. 故对于和 p 互素的整数 m，存在多项式，使得其所决定的除子恰好为 $< E[m] > -m^2 < O >$. 首先在特征为 0 上研究具有上述性质的多项式，然后在特征为 $p > 0$ 上验证已得的结论. 假设特征为 0.

定义 2.6.1 对于整数 $m \neq 0$，定义 m−th 可除多项式 (division polynomial) ψ_m 为由除子 $< E[m] > -m^2 < O >$ 和首项系数为 m 所唯一确定的有理函数. 令 $\psi_0 = 0$.

命题 2.6.2 对于正整数 m, n 有：

(1) $\psi_{-m} = -\psi_m$;

(2) $\psi_m^2 = m^2 \prod\limits_{P \in E[m] \setminus \{O\}} (X - X(P))$;

(3) $\psi_m \in \begin{cases} K[X], & m\text{是奇数}, \\ (2Y + a_1X + a_3)K[X], & m\text{是偶数}; \end{cases}$

(4) 如果 m,n 具有相同的奇偶性，则 $\psi_m\psi_n \in K[X]$.

证明 (1) 由 $E[m]=E[-m]$ 和定义 2.6.1 即得结论.

(2) 由 $\mathrm{div}(X-X(P)) = <P> + <\overline{P}> -2<O>$，可知左、右两边的有理函数决定了相同的除子；再注意到等式左、右两边的首项系数均为 m^2，则左、右两边相等.

(3) 如果 m 是奇数，则 $E[m]$ 中没有 2 阶点，所以存在 $S, S\cap\overline{S}$ 为空集，使得 $E[m]=S\dot{\cup}\overline{S}\dot{\cup}\{O\}$, 其中 $\overline{S}=\{\overline{P}:P\in S\}$，同上讨论即得 $\psi_m = m\prod_{P\in S}(X-X(P))$. 如果 m 是偶数，则可将 $E[m]$ 表示为 $S\dot{\cup}\overline{S}\dot{\cup}E[2]$，$\psi_m=\frac{m}{2}\psi_2\prod_{P\in S}(X-X(P))$. 已有 $\psi_2=2Y+a_1X+a_3$，将其代入即得结论.

(4) 由 (3) 知若 m,n 均为奇数，结论显然成立；若 m,n 均为偶数，只需证 $\psi_2^2\in K[X]$.

$$\begin{aligned}\psi_2^2 &= (2Y+a_1X+a_3)^2\\ &= 4Y^2+4Y(a_1X+a_3)+(a_1X+a_3)^2\\ &= 4(X^3+a_2X^2+a_4X+a_6)+(a_1X+a_3)^2\\ &\in K[X]\end{aligned}$$

命题 2.6.3 对于整数 $m\neq 0, n\neq 0$ 有 $g_m-g_n=-\dfrac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2}$.

证明 由命题 2.5.9 知左、右两边决定了相同的除子. 由命题 2.5.7 知左边的首项系数为 $\frac{1}{m^2}-\frac{1}{n^2}$，由定义 2.6.1 知右边的首项系数为 $-\frac{(m+n)(m-n)}{m^2n^2}$，所以左、右两边的有理函数相等.

命题 2.6.4 可除多项式是唯一满足下述递归关系的多项式：

$$\begin{aligned}&\psi_0=0,\\ &\psi_1=1,\\ &\psi_2=2Y+a_1X+a_3,\\ &\psi_3=3X^4+b_2X^3+3b_4X^2+3b_6X+b_8,\\ &\frac{\psi_4}{\psi_2}=2X^6+b_2X^5+5b_4X^4+10b_6X^3+10b_8X^2\\ &\qquad +(b_2b_8-b_4b_6)X+(b_4b_8-b_6^2).\end{aligned}$$

其中 b_i 的定义见上一章.

$$\psi_{m+n}\psi_{m-n} = \psi_n^2\psi_{m+1}\psi_{m-1} - \psi_m^2\psi_{n+1}\psi_{n-1}, \tag{2.2}$$

$$\psi_{2m} = \frac{\psi_m}{\psi_2}(\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2) \tag{2.3}$$

$$= (\psi_2 \circ [m])\psi_m^4, \tag{2.4}$$

$$\psi_{2m+1} = \psi_{m+2}\psi_m^3 - \psi_{m+1}^3\psi_{m-1}. \tag{2.5}$$

证明 对于 $m, n \neq 0$ ，由命题 2.6.3 即得式 (2.2), 因为 $g_m - g_n = (g_m - g_1) - (g_n - g_1)$ ，所以

$$\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2} = \frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2} - \frac{\psi_{n+1}\psi_{n-1}}{\psi_n^2}.$$

两边乘以 $\psi_m^2\psi_n^2$ 即得结论. 若 m, n 有一个为 0 ，则式 (2.2) 显然成立.

ψ_0, ψ_1, ψ_2 的表达式是显然的. 对于 ψ_3 ，令 $m = 2, n = 1$ ，利用命题 2.6.3 得 $\psi_3 = -(g_2 - X)\psi_2^2$ ，将 ψ_2 代入即得结论. 对于 ψ_4 ，令 $m = 3, n = 1$ ，同理得 $\psi_4 = -\dfrac{(g_3 - X)\psi_3^2}{\psi_2}$ ，将 ψ_3 代入即得结论. 以上说明可除多项式满足该递归关系及初始条件.

唯一性通过对式 (2.2) 取不同的 m, n 来证明. 令 $n = 0$, 则 $-\psi_m^2\psi_{-1} = \psi_m^2$ ，即 $\psi_{-1} = -1$; 令 $m = 0$, 则 $-\psi_n^2 = \psi_n\psi_{-n}$, 即 $\psi_{-n} = -\psi_n$; 设 $m \geqslant 3, n = 2$ ，则

$$\psi_{m+2} = \frac{\psi_2^2\psi_{m+1}\psi_{m-1} - \psi_m^2\psi_3}{\psi_{m-2}},$$

所以满足 $\psi_0, \psi_1, \psi_2, \psi_3, \psi_4$ 和递归关系的多项式列是唯一的.

在式 (2.2) 中将 m 替换为 $m+1$ ， n 替换为 $m-1$ ，即得式 (2.3) ；在式 (2.2) 中将 n 替换为 m,m 替换为 $m+1$ 即得式 (2.5) ；对于式 (2.4). 可以比较以下除子:

$$\mathrm{div}\psi_{2m} = < E[2m] > -4m^2 < O >,$$

$$\mathrm{div}\psi_m^4 = 4 < E[m] > -4m^2 < O >,$$

$$\begin{aligned}\mathrm{div}(\psi \circ [m]) &= \mathrm{div}([m]^*(\psi_2)) \\ &= [m]^*(\mathrm{div}\psi_2)\end{aligned}$$

$$\begin{aligned}
&= [m]^*(< E[2] > -4 < O >) \\
&= \sum_{P\in[m]^{-1}(E[2])} < P > -4 < E[m] > \\
&= < E[2m] > -4 < E[m] > .
\end{aligned}$$

所以 $\psi_{2m}, (\psi_2 \circ [m])\psi_m^4$ 决定了相同的除子. 比较双方的首项系数:

$$\begin{aligned}
l(\psi_{2m}) &= 2m, \\
l((\psi_2 \circ [m])\psi_m^4) &= l(2h_m + a_1 g_m + a_3)m^4 \\
&= \frac{2}{m^3} m^4 \\
&= l(\psi_{2m}).
\end{aligned}$$

所以 $\psi_{2m} = (\psi_2 \circ [m])\psi_m^4$.

推论 2.6.5 对于整数 m ，有 $\psi_m \in \mathbb{Z}[X, Y, a_1, a_3, a_2, a_4, a_6]/(E)$. 进一步，若 m 是奇数，则 $\psi_m \in \mathbb{Z}[X, a_1, a_3, a_2, a_4, a_6]/(E)$；若 m 是偶数，则 $\dfrac{\psi_m}{\psi_2} \in \mathbb{Z}[X, a_1, a_3, a_2, a_4, a_6]/(E)$.

证明 由命题 2.6.2 的证明知 $\psi_2^2 \in \mathbb{Z}[X, a_1, a_3, a_2, a_4, a_6]/(E)$. 用数学归纳法证明. 当 $m = 1, 2, 3$ 时结论显然成立. 若 $m \geqslant 5$ 是奇数，则利用 $\psi_2^2 \in \mathbb{Z}[X, a_1, a_3, a_2, a_4, a_6]/(E)$ 和式 (2.5) 即得结论. 若偶数 $m = 2k, k > 1$ ，则利用式 (2.3) ，并按 k 的奇、偶分情况讨论，同理可得结论.

命题 2.6.3 描述了 g_m, g_n 和可除多项式间的关系，即可利用可除多项式求取 g_m. 下面给出利用可除多项式计算 h_m 的方法：利用式 (2.3), 式 (2.4) 得

$$\begin{aligned}
2h_m + a_1 g_m + a_3 &= \psi_2 \circ [m] \\
&= \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{\psi_2\psi_m^3},
\end{aligned}$$

则可求得 h_m ，注意该方法不适用于 $p = 2$ ，但结论是通用的.

命题 2.6.6 设 m 是正整数，则 h_m 可以表述为:

(1)

$$h_m = \frac{\psi_{m+2}\psi_{m-1}^2 - \psi_{m-2}\psi_{m+1}^2}{2\psi_2\psi_m^3} - \frac{1}{2}(a_1 g_m + a_3);$$

(2)

$$h_m - Y = \frac{\psi_{m-2}\psi_{m+1}^2}{\psi_2\psi_m^3} + (3X^2 + 2a_2X + a_4 - a_1Y)\frac{\psi_{m-1}\psi_{m+1}}{\psi_2\psi_m^2} + \psi_2 \circ [m],$$

或等价地

$$h_m - Y = \frac{\psi_{m-1}^2\psi_{m+2}}{\psi_2\psi_m^3} + (3X^2 + 2a_2X + a_4 - a_1Y)\frac{\psi_{m-1}\psi_{m+1}}{\psi_2\psi_m^2}.$$

证明 (1) 显然成立;

令 $s' = 3X^2 + 2a_2X + a_4 - a_1Y$ ，用数学归纳法证明 (2) 中的第一个表达式. 通过简单计算可知对于 $m = 1, 2$ 结论成立. 设 $m > 2$ ，对于小于 m 的正整数结论均成立，证明对于 m 结论也成立. 利用加法公式得

$$h_m = -\frac{h_{m-1} - Y}{g_{m-1} - X}(g_m - X) - (a_1g_m + a_3 + Y),$$

所以

$$\begin{aligned} h_m - Y &= -\frac{g_m - X}{g_{m-1} - X}(h_{m-1} - Y) - \psi_2 \circ [m] + 2(h_m - Y) \\ \Leftrightarrow \quad h_m - Y &= \frac{g_m - X}{g_{m-1} - X}(h_{m-1} - Y) + \psi_2 \circ [m]. \end{aligned}$$

利用归纳假设和命题 2.6.3 得

$$\frac{g_m - X}{g_{m-1} - X}(h_{m-1} - Y) = \frac{\psi_{m+1}\psi_{m-1}^3}{\psi_{m-2}\psi_m^3}\left(\frac{\psi_m^2\psi_{m-3}}{\psi_2\psi_{m-1}^3} + s'\frac{\psi_m\psi_{m-2}}{\psi_2\psi_{m-1}^2} + \psi_2 \circ [m-1]\right).$$

由式 (2.3), 式 (2.4) 得

$$\psi_2 \circ [m-1] = \frac{\psi_{m+1}\psi_{m-2}^2 - \psi_{m-3}\psi_m^2}{\psi_2\psi_{m-1}^3},$$

代入得

$$\begin{aligned} \frac{g_m - X}{g_{m-1} - X}(h_{m-1} - Y) &= \frac{\psi_{m+1}\psi_{m-3}}{\psi_2\psi_{m-2}\psi_m} + s'\frac{\psi_{m+1}\psi_{m-1}}{\psi_2\psi_m^2} \\ &\quad + \frac{\psi_{m+1}^2\psi_{m-2}}{\psi_2\psi_m^3} - \frac{\psi_{m+1}\psi_{m-3}}{\psi_2\psi_{m-2}\psi_m} \\ &= \frac{\psi_{m+1}^2\psi_{m-2}}{\psi_2\psi_m^3} + s'\frac{\psi_{m+1}\psi_{m-1}}{\psi_2\psi_m^2}. \end{aligned}$$

将 $\psi_2 \circ [m]$ 用式 (2.3), 式 (2.4) 表示，即可证明 (2) 中的第二个表达式.

以下假设特征 p 是任意取值的.

推论 2.6.5 指出特征为 0 的条件下，可除多项式的系数属于 $\mathbb{Z}$，通过将其用模 p 作用，则可以定义特征为 p 的条件下的可除多项式. 如果本节已证明的各等式中的分母模 p 不为 0，则显然对于特征为 p 的可除多项式，各等式仍然成立. 为此，需要证明以下引理.

引理 2.6.7 如果 $m \neq 0$，则 $\psi_m \neq 0$.

证明 因为 $\psi_1 = 1, \psi_2 = 2Y + a_1X + a_3$，所以结论对于 $m = 1, 2$ 显然成立. 假设对于 $m > 2$ 的整数结论均成立. 由命题 2.6.3 得

$$\psi_m\psi_{m-2} = (X - g_{m-1})\psi_{m-1}^2.$$

由归纳假设知 $\psi_{m-2} \neq 0, \psi_{m-1} \neq 0$，而 $X \neq g_{m-1}$，所以 $\psi_m \neq 0$.

还需要证明如上定义的特征为 p 条件下的可除多项式所决定的除子仍然具有可除多项式定义中的性质，否则其定义失去了意义.

命题 2.6.8 如果 m 和 p 互素，则 $\mathrm{div}\psi_m = <E[m]> - m^2 <O>$.

证明 特征为 0 的条件下， $\mathrm{ord}_O\psi_m = -(m^2 - 1), l(\psi_m) = m$. 因为 m 和 p 互素，所以首项系数 m 模 p 后不为 0，故特征为 p 条件下， ψ_m 在 O 点的赋值仍为 $-(m^2 - 1)$，有 $m^2 - 1$ 个零点 (考虑重数). 在特征为 p 的条件下，仍有等式

$$g_m - X = -\frac{\psi_{m+1}\psi_{m-1}}{\psi_m^2}.$$

因为 $g_m - X$ 的所有有限极点恰好为 $E[m] \setminus \{O\}$， ψ_{m+1}, ψ_{m-1} 没有有限极点，所以 $E[m] \setminus \{O\}$ 中任一点一定是 ψ_m 的零点，而 $|E[m] \setminus \{O\}| = m^2 - 1$，$\deg(\mathrm{div}\psi_m) = 0$，故 ψ_m 的有限零点恰为 $E[m] \setminus \{O\}$，且各零点的阶为 1.

引理 2.5.12 的证明 在特征为 p 的条件下，因为 ψ_p 的首项系数模 p 为 0，所以 ψ_p 的有限零点个数小于 $p^2 - 1$. 同上分析可知 $E[p] \setminus \{O\}$ 的点均为 ψ_p 的零点，所以 $|E[p]| < p^2$.

例 2.5 设 $p \in \{2, 3\}, m$ 和 p 互素， $n = p^v n', v \geqslant 1, n'$ 和 p 互素，则由命题 2.5.9 知

$$\mathrm{div}(g_m - g_n) = <E[m+n]> + <E[m-n]> -2 <E[m]> -2\alpha^v <E[n]>.$$

另一方面，

$$g_m - g_n = -\frac{\psi_{m+n}\psi_{m-n}}{\psi_m^2\psi_n^2},$$

因为 $m, m+n, m-n$ 和 p 互素，则由命题 2.6.8 可知

$$\text{div}\psi_n = \alpha^v < E[n] > -\alpha^v |E[n]| < O > .$$

所以 ψ_n 的零点为 $E[n]$ 中的有限点，且阶为 α^v.

2.7 Weil 对

通常希望能够得到椭圆曲线在有限域上的点的个数，这是椭圆曲线的一个全局信息；通过研究 m 扭点，已经获得了局部信息，由局部转化为全体的任务将由 Weil 对 (Weil pairing) 来完成. 本节均假设 m 是和 p 互素的正整数.

在定义 Weil 对之前，先证明一个引理，它描述了自同态 $[m]$ 和域扩张 $K(E)/[m]^*(K(E))$ 间的关系.

引理 2.7.1 设有理函数 r 在 $E[m]$ 中点的移位作用下保持不动，则存在有理函数 s 使得 $r = s \circ [m]$，即 $r \in [m]^*(K(E))$.

证明 如果已有结论

$$\deg[m] = [K(E) : [m]^*(K(E))] \leqslant m^2, \tag{2.6}$$

则可以证明引理，令

$$J = [m]^*(K(E)) = \{t \circ [m] : t \in K(E)\},$$
$$H = \{r \in K(E) : r \circ \tau_S = r,\ \forall S \in E[m]\}.$$

显然 $J \subseteq H \subseteq K(E)$.$H$ 是 $K(E)$ 的 m^2 个自同态，即所有 m 扭点移位作用下的不动域，所以 $[K(E) : H] = m^2$. 由式 (2.6)，$m^2 = [K(E) : H] \geqslant [K(E) : J]$，所以式 (2.6) 等号成立，特别 $H = J$，即得所证结论.

下证式 (2.6)，考虑域 $K(g_m), K(g_m, h_m), K(X), K(E)$，注意 $J = K(X \circ [m], Y \circ [m]) = K(g_m, h_m)$. 因为 $\psi_m^2, \psi_{m-1}\psi_{m+1}$ 属于 $K[X]$(见命题 2.6.2)，所以再由命题 2.6.3 得

$$g_m - X = -\frac{\psi_{m-1}\psi_{m+1}}{\psi_m^2} \in K(X),$$

进一步有 $g_m \in K(X), K(g_m) \subseteq K(X)$(隐含了 $m\overline{P} = \overline{mP}$).

已有结论 $[K(E):K(X)]=2$. 计算 $[K(X):K(g_m)]$，由命题 2.6.3 知 X 满足 $K(g_m)[T]$ 中的多项式:

$$f(T)=T\psi_m^2(T)-(\psi_{m-1}\psi_{m+1})(T)-g_m\psi_m^2(T).$$

特征为 0 时，O 是 $\psi_m^2\in K[X]$ 的 $2(m^2-1)$ 阶极点，所以 ψ_m^2 的次数为 m^2-1. O 是 $\psi_{m-1}\psi_{m+1}$ 的 $(m-1)^2+(m+1)^2-2=2m^2$ 阶极点，所以 $\psi_{m-1}\psi_{m+1}$ 的次数为 m^2，故 $\deg\ f\leqslant m^2$. 在其余特征下，可除多项式的次数不会增加，所以对于任意特征，均有 $\deg\ f\leqslant m^2, [K(X):K(g_m)]\leqslant m^2$. 如果 $h_m\in K(g_m)$，则 $h_m\in K(X)$，意味着对于任意的 $P\in E$, 有 $Y(mP)=h_m(P)=h_m(\overline{P})=Y(\overline{mP})$，但 E 中存在 mP 不是 2 阶点，矛盾. 所以 $h_m\notin K(g_m), [K(g_m,h_m):K(g_m)]\geqslant 2$，

$$[K(E):J]=\frac{[K(E):K(X)][K(X):K(g_m)]}{[J:K(g_m)]}\leqslant\frac{2m^2}{2}=m^2.$$

对于 m 扭点 T 考虑一个特殊除子 $D=[m]^*(<T>-<O>)$. 显然除子 D 的次数为 0. 因为 $[m]$ 是满映射，不妨设 $T_0\in E, mT_0=T$，则

$$\begin{aligned}D&=\sum_{T'\in[m]^{-1}(T)}<T'>-\sum_{R\in\ker[m]}<R>\\&=\sum_{R\in E[m]}(<T_0+R>-<R>).\end{aligned}$$

$$\sum_{R\in E[m]}(T_0+R-R)=m^2T_0=mT=O.$$

所以 D 是主除子，即存在有理函数 g_T 使得 $\operatorname{div}\ g_T=[m]^*(<T>-<O>)$，但 g_T 并不唯一，彼此间相差一个非零常数.

定义 2.7.2 m 扭点上的 Weil 对定义为函数

$$\begin{aligned}e_m: E[m]\times E[m]&\to\mu,\\(S,T)&\mapsto\frac{g_T\circ\tau_S}{g_T},\end{aligned}$$

其中，μ 表示 K 中的所有 m-th 单位根组成的集合.

显然 $e_m(S,T)$ 与 g_T 的选取无关. 再由命题 2.2.4 可知

$$\begin{aligned}\operatorname{div}(g_T\circ\tau_S)&=\tau_S^*(\operatorname{div}\, g_T)\\&=\tau_S^*(\sum_{R\in E[m]}(<T_0+R>-<R>))\\&=\sum_{R\in E[m]}(<T_0+R-S>-<R-S>)\\&=\operatorname{div}\, g_T,\end{aligned}$$

则 $e_m(S,T)\in K.e_m(S,T)^m=1$ 将在后面证明.

命题 2.7.3 Weil 对具有下述性质:

(1) 双线性 (Bilinearity): $\forall S,S_1,S_2,T,T_1,T_2\in E[m]$,

$$\begin{aligned}e_m(S_1+S_2,T)&=e_m(S_1,T)e_m(S_2,T),\\e_m(S,T_1+T_2)&=e_m(S,T_1)e_m(S,T_2).\end{aligned}$$

(2) 恒等性 (Identity): $e_m(S,S)=1,\ \forall S\in E[m]$.

(3) 交错性 (Alternation): $e_m(S,T)=e_m(T,S)^{-1},\ \forall S,T\in E[m]$.

(4) 非退化性 (Non-degeneracy):

$$\begin{aligned}e_m(S,T)=1,\ \forall S\in E[m]\quad&\Leftrightarrow\quad T=O;\\e_m(S,T)=1,\ \forall T\in E[m]\quad&\Leftrightarrow\quad S=O.\end{aligned}$$

(5) 与自同态的相容性 (Compatibility): 设 α 是非零自同态, 则

$$e_m(\alpha(S),\alpha(T))=e_m(S,T)^{\deg\alpha}.$$

证明 (1) 直接计算:

$$\begin{aligned}e_m(S_1+S_2,T)&=\frac{g_T\circ\tau_{S_1+S_2}}{g_T}\\&=\frac{g_T\circ\tau_{S_1}\circ\tau_{S_2}}{g_T}\\&=(\frac{g_T\circ\tau_{S_1}}{g_T}\circ\tau_{S_2})\frac{g_T\circ\tau_{S_2}}{g_T}\\&=(e_m(S_1,T)\circ\tau_{S_2})e_m(S_2,T)\\&=e_m(S_1,T)e_m(S_2,T).\end{aligned}$$

要证明第二个等式，则必须在 $g_{T_1+T_2}$ 和 g_{T_1}, g_{T_2} 之间建立联系. 因为 $<T_1+T_2> - <T_1> - <T_2> + <O>$ 是主除子，所以存在有理函数 h ，使得 $\operatorname{div} h = <T_1+T_2> - <T_1> - <T_2> + <O>$ ，则

$$\begin{aligned}\operatorname{div}\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}} &= [m]^*(<T_1+T_2> - <T_1> - <T_2> + <O>)\\ &= [m]^*(\operatorname{div}\ h)\\ &= \operatorname{div}(h\circ[m]),\end{aligned}$$

因此存在 $c \in K^\times$ 使得

$$\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}} = ch\circ[m],$$

且在 $E[m]$ 点移位作用下其保持不动.

$$\begin{aligned}e_m(S, T_1+T_2) &= \left(\frac{g_{T_1+T_2}}{g_{T_1}g_{T_2}}\circ\tau_S\right)\frac{(g_{T_1}\circ\tau_S)(g_{T_2}\circ\tau_S)}{g_{T_1+T_2}}\\ &= \frac{g_{T_1}\circ\tau_S}{g_{T_1}}\cdot\frac{g_{T_2}\circ\tau_S}{g_{T_2}}\\ &= e_m(S,T_1)e_m(S,T_2).\end{aligned}$$

(2) 设 $S_0 \in E, mS_0 = S$ ，令 $G = \prod_{i=0}^{m-1}(g_S\circ\tau_{iS_0})$ ，则

$$\begin{aligned}\operatorname{div}(g_S\circ\tau_{iS_0}) &= \tau_{iS_0}^*(\operatorname{div}(g_S))\\ &= (\tau_{iS_0}^*\circ[m]^*)(<S> - <O>)\\ &= ([m]\circ\tau_{iS_0})^*(<S> - <O>)\\ &= (\tau_{iS}\circ[m])^*(<S> - <O>)\\ &= [m]^*(<S-iS> - <-iS>),\end{aligned}$$

$$\begin{aligned}\operatorname{div}\ G &= [m]^*\left(\sum_{i=0}^{m-1}(<(1-i)S> - <(0-i)S>)\right)\\ &= [m]^*\left(\sum_{i=2-m}^{1} <iS> - \sum_{i=1-m}^{0} <iS>\right)\\ &= [m]^*(<S> - <S-mS>)\\ &= 0.\end{aligned}$$

所以 G 是常值，且

$$
\begin{aligned}
1 &= \frac{G \circ \tau_{S_0}}{G} \\
&= \frac{g_S \circ \tau_{mS_0}}{g_S \circ \tau_{0S_0}} \\
&= \frac{g_S \circ \tau_S}{g_S} \\
&= e_m(S,S).
\end{aligned}
$$

(3) 直接计算得

$$
\begin{aligned}
1 &= e_m(S+T,S+T) \\
&= e_m(S,S)e_m(S,T)e_m(T,S)e_m(T,T) \\
&= e_m(S,T)e_m(T,S),
\end{aligned}
$$

结论显然成立.

(4) 由交错性知仅需证明第一个等式成立. 如果 $T=O$ ，则 g_T 是常值，所以 g_T 在移位作用下不动，故 $e_m(S,T)=1$. 如果对于任意的 $S\in E[m]$, 均有 $e_m(S,T)=1$ ，则 g_T 在 m 扭点移位作用下保持不动，由引理 2.7.1 知存在有理函数 r ，使得 $g_T = r\circ[m]$ ，

$$
\begin{aligned}
[m]^*(<T>-<O>) &= \operatorname{div} g_T \\
&= \operatorname{div}(r\circ[m]) \\
&= [m]^* \operatorname{div} r.
\end{aligned}
$$

因为 $[m]^*$ 是单射，所以 $\operatorname{div} r = <T>-<O>$ ， r 没有有限极点，故 r 是多项式，而 r 仅有一个有限零点，所以 r 是常值，则 $\operatorname{div} r = 0, T=O$.

(5) 设 T 是给定的 m 扭点，要证明对于任意 m 扭点 S ，有

$$
\frac{g_{\alpha(T)} \circ \tau_{\alpha(S)}}{g_{\alpha(T)}} = \left(\frac{g_T \circ \tau_S}{g_T}\right)^{\deg \alpha}
$$

因为左边是常值，所以左边与 α 复合，不改变取值：

$$
\begin{aligned}
\frac{g_{\alpha(T)} \circ \tau_{\alpha(S)}}{g_{\alpha(T)}} &= \frac{g_{\alpha(T)} \circ \tau_{\alpha(S)} \circ \alpha}{g_{\alpha(T)} \circ \alpha} \\
&= \frac{g_{\alpha(T)} \circ \alpha \circ \tau_S}{g_{\alpha(T)} \circ \alpha},
\end{aligned}
$$

右边为

$$\left(\frac{g_T \circ \tau_S}{g_T}\right)^{\deg \alpha} = \frac{g_T^{\deg \alpha} \circ \tau_S}{g_T^{\deg \alpha}}.$$

所以只需证对于任意 m 扭点 S 有

$$\frac{g_{\alpha(T)} \circ \alpha}{g_T^{\deg \alpha}} \circ \tau_S = \frac{g_{\alpha(T)} \circ \alpha}{g_T^{\deg \alpha}}.$$

由引理 2.7.1 知上式等价于存在有理函数 r ，使得

$$\frac{g_{\alpha(T)} \circ \alpha}{g_T^{\deg \alpha}} = r \circ [m],$$

计算得

$$\begin{aligned}
\operatorname{div}\left(\frac{g_{\alpha(T)} \circ \alpha}{g_T^{\deg \alpha}}\right) &= (\alpha^* \circ [m]^*)(< \alpha(T) > - < O >) \\
&\quad - \deg \alpha [m]^*(< T > - < O >) \\
&= [m]^*(\alpha^*(< \alpha(T) > - < O >) - \deg \alpha(< T > - < O >)) \\
&= [m]^*\Bigg(\sum_{R \in \ker \alpha} e_\alpha(< T + R > - < R >) \\
&\quad - \deg \alpha(< T > - < O >)\Bigg).
\end{aligned}$$

该除子的次数为 0 ，又因为

$$\begin{aligned}
\sum_{R \in \ker \alpha} e_\alpha(T + R - R) - \deg \alpha(T - O) &= (e_\alpha |\ker \alpha| - \deg \alpha) T \\
&= O,
\end{aligned}$$

所以该除子是主除子，即存在有理函数 r ，使得

$$\frac{g_{\alpha(T)} \circ \alpha}{g_T^{\deg \alpha}} = r \circ [m],$$

结论得证.

最后说明 $e_m(S,T)$ 是 m 次单位根：

$$\begin{aligned}
e_m(S,T)^m &= e_m(S, mT) \\
&= e_m(S, O) \\
&= 1.
\end{aligned}$$

2.8 Hasse 定理

定理 2.8.1 (Hasse) 设 $k=\mathbb{F}_q, t=q+1-|E(k)|$，则 Frobenius 自同态 φ 满足：

(1) $\varphi\circ\varphi-[t]\circ\varphi+[q]=[0]$;

(2) $|t|\leqslant 2\sqrt{q}$.

对于和 p 互素的整数 m， $E[m]\simeq\mathbb{Z}_m\times\mathbb{Z}_m$ 是秩为 2 的自由 $\mathbb{Z}_m$ 模.

引理 2.8.2 设 $\{T_1,T_2\}$ 是 $E[m]$ 作为 $\mathbb{Z}_m$ 模的一组基，则 $e_m(T_1,T_2)$ 是 m 次本原单位根.

证明 假设 $e_m(T_1,T_2)^n=1$, 则对于 $c_1,c_2\in\mathbb{Z}_m$ 有

$$\begin{aligned}e_m(nT_1,c_1T_1+c_2T_2)&=e_m(T_1,c_1T_1+c_2T_2)^n\\&=e_m(T_1,T_1)^{nc_1}e_m(T_1,T_2)^{nc_2}\\&=1,\end{aligned}$$

因为 $\{T_1,T_2\}$ 是基，所以 $c_1T_1+c_2T_2$ 跑遍 $E[m]$，再由 e_m 的非退化性得 $nT_1=O$，所以 $m|n$，而 $n|m$ 是显然的，故 $e_m(T_1,T_2)$ 是 m 次本原单位根.

下述定理将自同态的全局信息和该自同态限制在 $E[m]$ 上的局部信息间直接建立了联系，其证明利用了 Weil 对.

定理 2.8.3 设 α 是非零自同态，则 α 在 $E[m]$ 上的限制，记作 α_m，是线性自同态，且其行列式值为 $\deg\alpha \mod m$.

证明 显然 $\alpha(E[m])\subseteq E[m]$ 且 α_m 是线性的. 所以可将 $E[m]$ 作为 $\mathbb{Z}_m-$模， α_m 是定义好的 $E[m]$ 上的同态. 设 $\{T_1,T_2\}$ 是 $E[m]$ 的一组基，则 α_m 可由矩阵

$$\boldsymbol{A}=\begin{bmatrix}a_{11}&a_{12}\\a_{21}&a_{22}\end{bmatrix}$$

表示，其中 $\alpha_m(T_j)=a_{1j}T_1+a_{2j}T_2, j=1,2$. 则

$$\begin{aligned}e_m(T_1,T_2)^{\deg\alpha}&=e_m(\alpha(T_1),\alpha(T_2))\\&=e_m(a_{11}T_1+a_{21}T_2,a_{12}T_1+a_{22}T_2)\\&=e_m(T_1,T_1)^{a_{11}a_{12}}e_m(T_1,T_2)^{a_{11}a_{22}}e_m(T_2,T_1)^{a_{21}a_{12}}\end{aligned}$$

$$\begin{aligned}&e_m(T_2,T_2)^{a_{21}a_{22}}\\=&e_m(T_1,T_2)^{a_{11}a_{22}-a_{21}a_{12}}\\=&e_m(T_1,T_2)^{\det\alpha_m}.\end{aligned}$$

因为 $e_m(T_1,T_2)$ 是 m 次本原单位根，所以 $\det\alpha_m\equiv\deg\alpha \mod m$.

命题 2.8.4 设 α,β 是非零自同态， $c_1,c_2\in\mathbb{Z}$，则

$$\deg([c_1]\circ\alpha+[c_2]\circ\beta)=c_1^2\deg\alpha+c_2^2\deg\beta+c_1c_2(\deg(\alpha+\beta)-\deg\alpha-\deg\beta).$$

证明 设 m 是和 p 互素的充分大的整数，则左、右两边模 m 相等即为左、右两边相等，故可以将所有的自同态限制在 $E[m]$ 上来讨论.

注意：作为 $\mathbb{Z}$ 模的 $\mathrm{End}(E)$ 和作为 $\mathbb{Z}_m$ 模的 $\mathrm{End}(E)|_{E[m]}$ 有如下关系：

$$([c]\circ\alpha)_m=c\alpha_m.$$

由定理 2.8.3 得

$$\deg([c_1]\circ\alpha+[c_2]\circ\beta)=\det(c_1\alpha_m+c_2\beta_m)\mod m,$$

而

$$\begin{aligned}\det(c_1\alpha_m+c_2\beta_m)=&c_1^2\det\alpha_m+c_2^2\det\beta_m\\&+c_1c_2(\det(\alpha_m+\beta_m)-\det\alpha_m-\det\beta_m),\end{aligned}$$

再利用定理 2.8.3 即得结论.

域上 n 阶矩阵 $\boldsymbol{A}$的特征多项式 $f(x)$ 为

$$\det(xI-\boldsymbol{A})=x^n-\mathrm{Tr}(\boldsymbol{A})x+\det(\boldsymbol{A}),$$

有结论 $f(\boldsymbol{A})=0$.

命题 2.8.5 设 α 是自同态，则

$$\beta:=\alpha\circ\alpha-[1+\deg\alpha-\deg([1]-\alpha)]\circ\alpha+[\deg\alpha]=[0].$$

证明 同前将所有的自同态均限制在 $E[m]$ 上讨论，其中 $m\neq p$ 是素数，则

$$\beta_m=\alpha_m^2-(1+\det\alpha_m-\det(id-\alpha_m))\alpha_m+\det\alpha_m.$$

而 $\mathrm{Tr}\alpha_m = 1 + \det\alpha_m - \det(id - \alpha_m)$ ，所以 $\beta_m = 0$. 随着 m 的不同，则对于无限多的扭点 P 有 $\beta(P) = O$. 若 $\beta = (\beta_1, \beta_2)$ ， β_1, β_2 均为有理函数，则 β_1, β_2 仅有有限多个极点，所以使得 $\beta(P) = O$ 的 P 点的个数有限，矛盾，故 $\beta = [0]$.

定理 2.8.1 的证明 注意 k 是 $x \mapsto x^q$ 的不动域，所以

$$
\begin{aligned}
E(k) &= \{(x,y) \in E : (x^q, y^q) = (x,y)\} \cup \{O\} \\
&= \{P \in E : \varphi(P) = P\} \\
&= \ker([1] - \varphi).
\end{aligned}
$$

由推论 2.4.5 知 $[1] - \varphi$ 可分，则

$$\deg([1] - \varphi) = |\ker([1] - \varphi)| = |E(k)|.$$

已有结论 $\deg\varphi = q$ ，在命题 2.8.5 中令 $\alpha = \varphi$ 即得定理的第一部分.

对于任意的 $c_1, c_2 \in \mathbb{Z} \setminus \{0\}$ ，有

$$c_1^2 + c_2^2 q - c_1 c_2 t = \deg([c_1] \circ [1] + [c_2] \circ (-\varphi)) \geqslant 0.$$

除以 c_2^2 得

$$\left(\frac{c_1}{c_2}\right)^2 - \frac{c_1}{c_2} t + q \geqslant 0,$$

即对于所有的 $r \in \mathbb{Q}$ 有

$$r^2 - rt + q \geqslant 0,$$

则该不等式在 $\mathbb{R}$ 中也成立，所以其判别式 $t^2 - 4q \leqslant 0$ ，即得 $t^2 \leqslant 4q$.

2.9 群 结 构

$k = \mathbb{F}_q$ 上椭圆曲线 E 的阶一旦确定，其群结构比较简单. 由 Abelian 群基本定理 2.5.11 知 $E(k)$ 同构于循环群的直积

$$\mathbb{Z}_{n_1} \times \cdots \times \mathbb{Z}_{n_r},$$

其中， $n_1 > 1, n_i | n_{i+1}, i = 1, \cdots, r-1$. 因为 $E(k)$ 是有限群，所以存在整数 m 使得 $E(k) \subseteq E[m]$. 又由定理 2.5.4 知 $E[m]$ 同构于 $\mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}, m_1, m_2$ 为正整数，则 $r \leqslant 2$.

定理 2.9.1 (Rück) 设 E 是 $\mathbb{F}_q$ 上的椭圆曲线，则

$$E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}$$

其中， $n_1|n_2, n_1|q-1$.

证明 令 $k = \mathbb{F}_q$. 只需证 $n_1|q-1$. 因为 $n_1|n_2$ ，所以 $E(k)$ 包含子群 $\mathbb{Z}_{n_1} \times \mathbb{Z}_{n_1}$ ，故 $E(k)$ 有 n_1^2 个 n_1 扭点. 由定理 2.5.4 知， $E(k)$ 包含了所有的 n_1 扭点. 又由引理 2.8.2 知，存在 $P, Q \in E[n_1] \subseteq E(k)$ ，使得 $e_{n_1}(P,Q)$ 是 n_1−th 单位根. 令 φ 表示 $E(k)$ 的 Frobenius 自同态，则 $\varphi(P) = P, \varphi(Q) = Q$ ，故

$$\begin{aligned} e_{n_1}(P,Q) &= e_{n_1}(\varphi(P), \varphi(Q)) \\ &= e_{n_1}(P,Q)^{\deg\varphi} \\ &= e_{n_1}(P,Q)^q, \end{aligned}$$

因此 $e_{n_1}(P,Q) \in k, n_1|q-1$.

2.10 Weil 定理

设 $L = \mathbb{F}_{q^e}$ 是 $k = \mathbb{F}_q$ 的 e 次扩张，已知 $|E(k)|$ ，则可以求得 $|E(L)|$. 当 k 较小时，可以穷举来获得 $|E(k)|$.

设 $|E(k)| = q+1-t, |E(L)| = q^e+1-t_e$ ，由 Hasse 定理知 $\varphi_k : (x,y) \mapsto (x^q, y^q)$ 是多项式 $T^2 - sT + q \in \mathbb{Z}[T]$ 在 $\mathrm{End}(E)$ 中的零点. 同理，自同态 $\varphi_L : (x,y) \mapsto (x^{q^e}, y^{q^e})$ 是 $T^2 - tT + q^e$ 的零点. 对于 $t' \neq t$ ， φ_L 不满足方程 $T^2 - t'T + q^e$ ：如果满足，则有 $[0] = [t'-t] \circ \varphi_L$ ，又因为 φ_L 是满映射，故 $[t'-t] = [0], t' = t$. 由于 $\varphi_L = \varphi_k^e$, 所以 t 是唯一的整数使得 φ_k 是 $T^{2e} - tT^e + q^e$ 的零点.

对于 $T^2 - sT + q$ ，其判别式 $D = s^2 - 4q$ ，由 Hasse 定理知 $D \leqslant 0$. 设 α, β 是 $T^2 - sT + q$ 在复数域中的零点，则 α, β 是共轭的. 因为

$$\begin{aligned} t_e &= \alpha^e + \beta^e \\ &= \alpha^e + \alpha^{e-1}\beta + \beta^e + \alpha\beta^{e-1} - (\alpha^{e-1}\beta + \alpha\beta^{e-1}) \\ &= tt_{e-1} - qt_{e-2} \in \mathbb{Z}, \end{aligned}$$

所以多项式

$$f(T) = T^{2e} - (\alpha^e + \beta^e)T^e + q^e \in \mathbb{Z}[T].$$

又因为 $\alpha\beta=q$，所以 $f(\alpha)=f(\beta)=0$. 如果 $D<0$，则 α,β 是 f 的两个不同的根，因此在 $\mathbb{Z}[T]$ 中有 $T^2-sT+q=(T-\alpha)(T-\beta)$ 整除 f，则 φ_k 是 f 的零点. 如果 $D=0$，则 $f'(T)=2eT^{e-1}(T^e-\alpha^e), f'(\alpha)=0$，故 $\alpha=\beta$ 是 f 的二重根，同上可知 φ_k 是 f 的零点. 所以 $t=\alpha^e+\beta^e$，由此可得下述定理.

定理 2.10.1 (Weil) 设 E 定义在 $\mathbb{F}_q$ 上，$|E(\mathbb{F}_q)|=q+1-t, m$ 是正整数，在复数域中 T^2-tT+q 分解为 $(T-\alpha)(T-\beta)$，则

$$|E(\mathbb{F}_{q^e})|=q^e+1-(\alpha^e+\beta^e).$$

例 2.6 $Y^2+Y=X^3+X+1$ 定义在 $\mathbb{F}_2$ 上，直接计算得 $E(\mathbb{F}_2)=\{O\}, s=2$，因为

$$T^2-2T+2=(T-(1+i))(T-(1-i)),$$

所以

$$\begin{aligned}|E(\mathbb{F}_{2^m})|&=2^m+1-((1+i)^m+(1-i)^m)\\&=2^m+1-\begin{cases}2\cdot(-4)^{\frac{m}{4}}, & m\equiv 0(\mathrm{mod}\ 4),\\0, & m\equiv 2(\mathrm{mod}\ 4),\\2\cdot(-4)^{\frac{m-1}{4}}, & m\equiv 1(\mathrm{mod}\ 4),\\(-4)^{\frac{m+1}{4}}, & m\equiv 3(\mathrm{mod}\ 4),\end{cases}\end{aligned}$$

特别地，$m=2$ 时有 $|E(\mathbb{F}_4)|=5$.

2.11 扭 曲 线

如果已知定义在 $k=\mathbb{F}_q$ 上椭圆曲线 E 的阶，则很容易给出另一条曲线 E'，使得 $E(k)$ 中点的 X 坐标和 k 中非 $E'(k)$ 中点的 X 坐标间存在双映射，那么若 $|E'(k)|=q+1+t$，则 $|E(k)|=q+1-t$. 首先分析对于给定的 $x\in k$，如何判断其是否是 $E(k)$ 中点的 X 坐标.

命题 2.11.1 设 $Y^2+aY+b\in k[Y]$ 是二次方程：

(1) 如果 $p\neq 2$，则该方程在 k 中有根，当且仅当下述等价说法之一成立：

① a^2-4b 为 0，或是 k 中的二次剩余.

② $\gcd(Y^2+aY+b, Y^q-Y)\neq 1$.

(2) 如果 $p=2, q=2^m$，定义 k 的迹函数 (trace function) 为

$$\mathrm{Tr}: k \to \mathbb{F}_2,$$
$$x \mapsto \sum_{i=0}^{m-1} x^{2^i}.$$

则该方程在 k 中有根，当且仅当 $a=0$ 或 $\mathrm{Tr}(a^{-2}b)=0$.

证明　(1) 因为

$$\sigma: k^\times \to k^\times,$$
$$x \mapsto x^2,$$

是乘法群同态，其核为 $\{\pm 1\}$，所以 σ 的像集是 $k^\times$ 的子群，其指数为 2，该子群中的元素称为二次剩余 (quadratic residue). 则 $k^\times \setminus \sigma(k^\times)$ 由所有的二次非剩余 (quadratic non-residue) 组成. 引入二次特征 (quadratic character)

$$\chi: k^\times \to \{\pm 1\},$$
$$x \mapsto \begin{cases} 1, & x\text{是二次剩余}, \\ -1, & x\text{是二次非剩余}. \end{cases}$$

令 $\chi(0)=0$，则将 χ 扩展为 k 上的乘性函数. 对所给方程配方可得

$$Y^2+aY+b=\left(Y+\frac{a}{2}\right)^2-\frac{a^2-4b}{4},$$

所以该方程在 k 中有根当且仅当 $\chi(a^2-4b)\neq -1$.

由

$$Y^q-Y=\prod_{y\in k}(Y-y),$$

知

$$\gcd(Y^2+aY+b, Y^q-Y)=\prod_{y\in k: y^2+ay+b=0}(Y-y),$$

所以该方程在 k 中有根当且仅当 $\gcd(Y^2+aY+b, Y^q-Y)\neq 1$.

(2) $a=0$ 时方程一定有根. 若方程有根且 $a\neq 0$，通过变量替换 $Y\mapsto aY$，再除以 a^2，可得二次方程 $Y^2+Y+\dfrac{b}{a^2}$，所以不妨设所给的二次方程中的 $a=1$. 设 y 是 $Y^2+Y=b$ 在 k 中的一个根，不断地对 $y^2+y=b$ 平方得

$$y^{2^i}+y^{2^{i-1}}=b^{2^{i-1}}, \qquad 1\leqslant i\leqslant m,$$

将它们相加，即得 $0 = y^{2^m} + y = \mathrm{Tr}\ b$. 所以 $Y^2 + Y + b$ 在 k 中有根，则 $\mathrm{Tr}\ b = 0$. 另一方面，如果 y 是该方程的根，则 $y+1$ 也是根，所以在 k 中有根的方程 $Y^2 + Y = b$ 共有 $\frac{q}{2}$ 个. 而使得 $\mathrm{Tr}\ b = 0$ 的方程 $Y^2 + Y = b$ 也共有 $\frac{q}{2}$ 个，故方程 $Y^2 + Y = b$ 在 k 中有根当且仅当 $\mathrm{Tr}\ b = 0$.

以下分情况讨论 E' 的构造. 设 $p \neq 2, E$ 为正规型

$$Y^2 = s(X), \qquad s(X) = X^3 + a_2X^2 + a_4X + a_6.$$

则由引理的证明知

$$\begin{aligned}|E(k)| &= |E(k) \setminus \{O\}| + 1 \\ &= \sum_{x\in k}(\chi(4s(x)) + 1) + 1 \\ &= q + 1 + \chi(2)^2 \sum_{x\in k} \chi(s(x)) \\ &= q + 1 + t,\end{aligned}$$

其中 $t = \sum_{x\in k} \chi(s(x))$.

给定二次非剩余 $\gamma \in k$ ，定义

$$E' : Y^2 = s'(X), s'(X) = X^3 + \gamma a_2 X^2 + \gamma^2 a_2 X + \gamma^3 a_6,$$

则 $s'(\gamma x) = \gamma^3 s(x)$ 且

$$\begin{aligned}|E'(k)| &= q + 1 + \sum_{x\in k} \chi(s'(x)) \\ &= q + 1 + \sum_{x\in k} \chi(s'(\gamma x)) \\ &= q + 1 + \chi(\gamma)^3 \sum_{x\in k} \chi(s(x)) \\ &= q + 1 - t.\end{aligned}$$

设 $p = 2$ ，考虑一般的椭圆曲线方程

$$E : Y^2 + (a_1X + a_3)Y = s(X), s(X) = X^3 + a_2X^2 + a_4X + a_6, a_1X + a_3 \neq 0,$$

由引理可知

$$|E(k)| = |E(k) \setminus E[2]| + |E(k) \cap E[2]|$$

$$= 2|\{x \in k : a_1x + a_3 \neq 0, Tr((a_1x + a_3)^{-2}s(x)) = 0\}| + |E(k) \cap E[2]|.$$

因为 $E[2] \subseteq E(k)$ 且

$$|E[2]| = \begin{cases} 1, & a_1 = 0 \\ 2, & a_1 \neq 0 \end{cases} = |\{x \in k : a_1x + a_3 = 0\}| + 1.$$

令 $\gamma \in k$ 是迹为 1 的元素,

$$E' : y^2 + (a_1X + a_3)Y = s'(X), s'(X) = s(X) + \gamma(a_1X + a_3)^2,$$

则

$$\begin{aligned}
\mathrm{Tr}((a_1x + a_3)^{-2}s'(x)) &= \mathrm{Tr}((a_1x + a_3)^{-2}s(x) + \gamma) \\
&= \mathrm{Tr}((a_1x + a_3)^{-2}s(x)) + 1, \\
|E(k)| + |E'(k)| &= 2|\{x \in k : a_1x + a_3 \neq 0, \mathrm{Tr}((a_1x + a_3)^{-2}s(x)) = 0\}| \\
&\quad +2|\{x \in k : a_1x + a_3 \neq 0, \mathrm{Tr}((a_1x + a_3)^{-2}s(x)) = 1\}| \\
&\quad +2|E[2]| \\
&= 2|\{x \in k : a_1x + a_3 \neq 0\}| + 2(|x \in k : a_1x + a_3 = 0\}| + 1) \\
&= 2(q + 1).
\end{aligned}$$

故若 $|E(k)| = q + 1 + t$ ，则 $|E'(k)| = q + 1 - t$.

定义 2.11.2 设 E 是 k 上的椭圆曲线，如下定义椭圆曲线 E'：

(1) 若 $p \neq 2, E : Y^2 = X^3 + a_2X^2 + a_4X + a_6, \gamma \in k$ 是二次非剩余，则

$$E' : Y^2 = X^3 + \gamma a_2X^2 + \gamma^2 a_4X + \gamma^3 a_6.$$

(2) 若 $p = 2, E : Y^2 + (a_1X + a_3)Y = X^3 + a_2X^2 + a_4X + a_6, \gamma \in k, \mathrm{Tr}\gamma = 1$ ，则

$$E' : Y^2 + (a_1X + a_3)Y = X^3 + (a_2 + \gamma a_1^2)X^2 + a_4X + (a_6 + \gamma a_3^2).$$

E' 称为 E 的 γ 扭曲线 (twist by γ).

扭曲线是对称的，即 E' 是 E 的 γ 扭曲线，则 E 是 E' 的 γ' 扭曲线，其中若 $p \neq 2$ ， $\gamma' = \gamma^{-1}$ ；若 $p = 2$ ， $\gamma' = \gamma$. 显然 E 的扭曲线不唯一，若 $p \neq 2$ ，

k 中有 $\frac{q-1}{2}$ 个二次非剩余；若 $p=2$， k 中有 $\frac{q}{2}$ 个迹为 1 的元素，所以对于 $p\neq 2$ 和 $p=2$， E 分别有 $\frac{q-1}{2}$ 和 $\frac{q}{2}$ 个扭曲线.

命题 2.11.3 如果 $|E(k)|=q+1+t$, 则对 E 的 γ 扭曲线 E' 有 $|E(k')|=q+1-t$.

命题 2.11.4 设 E 是定义在 k 上的椭圆曲线，则 E 的所有二次非剩余，或迹为 1 的元素决定的扭曲线是 k 同构的，因此“扭”定义了椭圆曲线的 k 同构类间的一个双映射.

这里 k 同构是指存在系数属于 k 的可允许变换，使得将一个 E 的扭曲线转换为另一个 E 的扭曲线.

证明 (1) 若 $p\neq 2, E: Y^2=X^3+a_2X^2+a_4X+a_6$. 因为 E 的两条不同的二次非剩余扭曲线的差距是一条二次剩余决定的形如扭曲线方程的曲线，所以只需要证明如果 $\gamma=\delta^2\in k$, 则

$$E'': Y^2=X^3+\gamma a_2X^2+\gamma^2a_4X+\gamma^3a_6$$

同构于 E. 显然可允许变换

$$(X,Y)\mapsto(\gamma^{-1}X,(\gamma\delta)^{-1}Y)$$

将 E 转换为 E'.

(2) 若 $p=2, E: Y^2+(a_1X+a_3)Y=X^3+a_2X^2+a_4X+a_6$，同理只需证明对于迹为 0 的元素 $\gamma\in k$,

$$E'': Y^2+(a_1X+a_3)Y=X^3+(a_2+\gamma a_1^2)X^2+a_4X+(a_6+\gamma a_3^2)$$

同构于 E.

因为 $\mathrm{Tr}(\gamma)=0$，所以存在 $s,t\in k$ 使得

$$s^2+a_1s+\gamma a_1^2=0,\qquad t^2+a_3t+\gamma a_3^2=0.$$

可允许变换 $(X,Y)\mapsto(X,Y+sX+t)$ 将 E 转换为 $E''+(a_3s+a_1t)X$. 由 s,t 满足的方程得

$$(a_3s+a_1t)^2=a_1a_3(a_3s+a_1t).$$

如果 $a_3s+a_1t\neq 0$，则 $a_3s+a_1t=a_1a_3$，将 s 用 $X^2+a_1X+\gamma a_1^2$ 的另一个根 $s'=s+a_1$ 替换，有 $a_3s'+a_1t=(a_3s+a_1t)+a_1a_3=0$，故可允许变换 $(X,Y)\mapsto(X,Y+s'X+t)$ 将 E 转换为 E''.

2.12 超奇异曲线

超奇异曲线 (supersingular curve) 是一类特殊的椭圆曲线，其阶和群结构容易确定. 本节将讲述这类曲线的一些性质，由于大部分结论的证明利用了函数域、Abel 簇 (Abelian varieties) 的理论，超出了本书的范围，故只给出结论，证明可以参看有关参考书.

定义 2.12.1 椭圆曲线 E 称为超奇异的，如果 E 中没有 p 阶点，即 $E[p]=\{O\}$.

由命题 2.5.5 可知：

定理 2.12.2 若 $p=2,3$，则 E 是超奇异的，当且仅当 $j(E)=0$.

在 Waterhouse 的博士论文中，作者给出了有限域上椭圆曲线的阶的可能取值，即对于这些数，一定存在有限域上的椭圆曲线，使得其阶恰为该数. 其证明参看文献 [141]p.536.

定理 2.12.3 (Waterhouse) 设 $k=\mathbb{F}_q=\mathbb{F}_{p^m}$, 整数 $t\leqslant 2\sqrt{q}$，则存在定义在 k 上的椭圆曲线 E 且 $|E(k)|=q+1-t$，当且仅当下述条件之一满足：

(1) p 与 t 互素.

(2) m 是偶数，且

① $t=\pm 2\sqrt{q}$;

② $t=\pm\sqrt{q}$ 且 $p\not\equiv 1 \mod 3$;

③或 $t=0$ 且 $p\not\equiv 1 \mod 4$.

(3) m 是奇数，且

① $t=0$;

② $t=\pm\sqrt{2q}$ 且 $p=2$;

③或 $t=\pm\sqrt{3q}$ 且 $p=3$.

第一种情况下，椭圆曲线是非超奇异的；后两种情况下，椭圆曲线是超奇异的.

推论 2.12.4 有限域 $k=\mathbb{F}_q$ 上的椭圆曲线 E 是超奇异的，当且仅当

$$p|q+1-|E(k)|.$$

下述定理给出了超奇异椭圆曲线的群结构.

定理 2.12.5 设 E 是有限域 $k=\mathbb{F}_q$ 上的超奇异椭圆曲线，$t=q+1-|E(k)|$，则 $E(k)$ 的群结构如下：

(1) 若 $t^2\in\{q,2q,3q\}$，则 $E(k)$ 是循环群.

(2) 若 $t=\pm 2\sqrt{q}$，则 $E(k)\simeq \mathbb{Z}_{\sqrt{q}\pm 1}\times \mathbb{Z}_{\sqrt{q}\pm 1}$.

(3) 若 $t=0, q\not\equiv -1 \mod 4$，则 $E(k)$ 是循环群；若 $t=0, q\equiv -1 \mod 4$，则 $E(k)$ 为循环群或形如 $\mathbb{Z}_2\times\mathbb{Z}_{\frac{q+1}{2}}$.

证明 令 k 的特征为 p. 由定理 2.9.1 知 $E(k)\cong \mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}, n_1|n_2, n_1|q-1$，特别地，$E[n_1]\subseteq E(k), \gcd(n_1,p)=1$. 因为 $n_1^2|q+1-t$，所以 $n_1|t-2$. 设 $t^2=aq$，则 $a=0,1,2,3,4$. 因为 $n_1|q-1$，所以 $n_1|t^2-a$，即 $n_1|\gcd(t-2,t^2-a)$.

(1) 若 $a=3$，则 $n_1=1$，结论成立.

(2) 若 $a=2$，则 $n_1|2$. 因为此时 k 的特征 $p=2$，而 $\gcd(n_1,p)=1$，故 $n_1=1$. 结论成立.

(3) 若 $a=1$，则 $n_1|3$. 如果 $n_1=3$，因为 $n_1|t-2$，所以 $3|\sqrt{q}-2$，即 $3|\sqrt{q}+1$，则 $9|q+1+2\sqrt{q}$. 又因为 $n_1^2|q+1-t$，即 $9|q+1-\sqrt{q}$，所以 $3|\sqrt{q}$ 和 $\gcd(n_1,p)=1$ 矛盾. 故 $n_1=1$. 结论成立.

(4) 若 $a=0$，则 $n_1|2$. 如果 $n_1=2$，则有 $4=n_1^2|q+1$，即 $q\equiv -1 \mod 4$. 所以若 $q\not\equiv -1 \mod 4$，有 $n_1=1$，即 $E(k)$ 是循环群. 若 $q\equiv -1 \mod 4$，则 $n_1=1$或2，即 $E(k)$ 为循环群或同构于 $\mathbb{Z}_2\times\mathbb{Z}_{\frac{q+1}{2}}$.

(5) $a=4$ 的情况作为练习 (见习题 2.8).

定理 2.12.6 设 E 是有限域 $k=\mathbb{F}_q$ 上的超奇异椭圆曲线，n 是 $E(k)$ 中任意一点的阶，则 $E[n]\subseteq E(\mathbb{F}_{q^c})$，其中 $c\leqslant 6$.

在文献 [117] 中，Schoof 还给出了对应于 t 的非同构椭圆曲线的个数 $N(t)$. 设 $\Delta<0, \Delta\equiv 0,1 \mod 4$，则令

$$\Omega=\{aX^2+bXY+cY^2: a,b,c\in\mathbb{Z}, b^2-4ac=\Delta, a>0\};$$

$$G=SL(2,\mathbb{Z})=\left\{\begin{pmatrix} p & q\\ r & s\end{pmatrix}: p,q,r,s\in\mathbb{Z}, ps-rq=1\right\}.$$

对于任意的

$$\sigma=\begin{pmatrix} p & q\\ r & s\end{pmatrix}\in G,$$

$$f(X,Y)=aX^2+bXY+cY^2\in\Omega,$$

σ 对 $f(X,Y)$ 的作用定义为

$$\sigma(f(X,Y))=a(pX+qY)^2+b(pX+qY)(rX+sY)+c(rX+sY)^2,$$

则 $\sigma(f(X,Y)) \in \Omega.\Omega/G$ 中等价类的个数称为 Kronecker 类数，记作 $H(\Delta)$，即 $H(\Delta) = |\Omega/G|$.

定理 2.12.6 (Schoof) 设 $k = \mathbb{F}_q = \mathbb{F}_{p^m}$，$N(t)$ 表示满足 $q+1-|E(k)| = t$ 的定义在 k 上的非同构椭圆曲线 E 的个数，$\left(\dfrac{a}{p}\right)$ 表示 Legendre 符号，则对于 $|t| \leqslant 2\sqrt{q}$，有：

(1) 若 t, p 互素，则 $N(t) = H(t^2 - 4q)$；

(2) 若 m 是偶数，则

$$N(\pm 2\sqrt{q}) = \frac{1}{12}\left(p + 6 - 4\left(\frac{-3}{p}\right) - 3\left(\frac{-4}{p}\right)\right),$$
$$N(\pm\sqrt{q}) = 1 - \left(\frac{-3}{p}\right),$$
$$N(0) = 1 - \left(\frac{-4}{p}\right);$$

(3) 若 m 是奇数，则

$$N(0) = H(-4p),$$
$$N(\pm\sqrt{pq}) = 1, \qquad p = 2, 3.$$

对于偶特征，Menezes 和 Vanstone 对上述定理给出了初等证明，并决定了每一个等价类的代表元 [85]. 表 2.4 罗列了 m 为偶数时超奇异曲线的等价类的代表元. γ 非三次 (non-cube) 剩余，$\omega, \alpha, \beta, \delta \in \mathbb{F}_{2^m}$，

$$\mathrm{Tr}\omega = \mathrm{Tr}(\gamma^{-2}\alpha) = \mathrm{Tr}(\gamma^{-4}\beta) = 1,$$
$$\mathrm{Tr}_{\mathbb{F}_4}\delta \neq 0,$$

其中

$$\mathrm{Tr}\kappa = \sum_{i=0}^{m-1} \kappa^{2^i},$$
$$\mathrm{Tr}_{\mathbb{F}_4}\kappa = \sum_{i=0}^{\frac{m}{2}-1} \kappa^{4^i}.$$

t 栏中 $\dfrac{m}{2}$ 为偶数时，上面的符号有效；$\dfrac{m}{2}$ 为奇数时，下面的符号有效. 表 2.5 给出了 m 为奇数时，超奇异曲线的代表元，t 栏中 $m \equiv \pm 1 \mod 8$ 时，上面的符号有效；$m \equiv \pm 3 \mod 8$ 时，下面的符号有效.

利用类似的方法，Morain 针对特征为 3 的情况，将超奇异曲线进行了分类. 表 2.6 、表 2.7 分别罗列了文献 [94] 中 m 为偶数、奇数的结果. γ 是二次非剩余，$\delta \in k$ 迹为 1. 当 $\frac{m}{2}\left(\frac{m-1}{2}\right)$ 为偶数时，上面的符号有效；当 $\frac{m}{2}\left(\frac{m-1}{2}\right)$ 为奇数时，下面的符号有效.

表 2.4　m为偶数，$\mathbb{F}_{2^m}$上超奇异椭圆曲线的等价类

代表元	t
$Y^2+\gamma Y=X^3$	$\pm\sqrt{q}$
$Y^2+\gamma Y=X^3+\alpha$	$\mp\sqrt{q}$
$Y^2+\gamma^2 Y=X^3$	$\pm\sqrt{q}$
$Y^2+\gamma^2 Y=X^3+\beta$	$\mp\sqrt{q}$
$Y^2+Y=X^3+\delta X$	0
$Y^2+Y=X^3$	$\mp 2\sqrt{q}$
$Y^2+Y=X^3+\omega$	$\pm 2\sqrt{q}$

表 2.5　m为奇数，$\mathbb{F}_{2^m}$上超奇异椭圆曲线的等价类

代表元	t
$Y^2+Y=X^3$	0
$Y^2+Y=X^3+X$	$\pm\sqrt{2q}$
$Y^2+Y=X^3+X+1$	$\mp\sqrt{2q}$

表 2.6　m为偶数，$\mathbb{F}_{3^m}$上超奇异椭圆曲线的等价类

代表元	t
$Y^2=X^3-X$	$\pm 2\sqrt{q}$
$Y^2=X^3-\gamma^2 X$	$\mp 2\sqrt{q}$
$Y^2=X^3-\gamma X$	0
$Y^2=X^3-\gamma^3 X$	0
$Y^2=X^3-X+\delta$	$\mp\sqrt{q}$
$Y^2=X^3-\gamma^2 X+\gamma^3\delta$	$\pm\sqrt{q}$

表 2.7　m为奇数，$\mathbb{F}_{3^m}$上超奇异椭圆曲线的等价类

代表元	t
$Y^2=X^3+X$	0
$Y^2=X^3-X$	0
$Y^2=X^3-X+\delta$	$\mp\sqrt{3q}$
$Y^2=X^3-X-\beta$	$\mp\sqrt{3q}$

习 题 二

2.1 设 α, β 是 E 到 E' 上的两个有理映射，基域特征为 2 或 3，则

$$(\alpha+\beta)(P)=\alpha(P)+\beta(P), \qquad \forall P \in E.$$

2.2 设 $\alpha=(\alpha_1,\alpha_2)\in E'(K(E))$ 是偶有理映射，则 α_1,α_2 一定有形式

$$\alpha_1 = \frac{a}{c^2},$$
$$\alpha_2 = \frac{b}{c^3},$$

其中 $a,b,c\in K[X]$.

2.3 设 $k\in K$ 且不存在 $l\in K$ 使得 $l^p=K$，则对于任意的整数 $e\geqslant 0$ 有 $X^{p^e}-k$ 在 $K[X]$ 中不可约.

2.4 设 m 是正整数，证明：

(1) $g_m\in K(X)$;

(2) $\deg[m]\leqslant m^2$.

2.5 设 $p\in\{2,3\}$，对于任意 $m\in\mathbb{N}$，计算 $l(g_m), l(h_m)$.

2.6 设 $P\in E[m]$，则 $\mathrm{ord}_P g_m=\mathrm{ord}_O g_m$.

2.7 设 m,n 是非零整数，$p\neq 2,3$ 且 $m,n,m+n,m-n$ 均与 p 互素，则

$$\mathrm{div}(g_m-g_n)=<E[m+n]>+<E[m-n]>-2<E[m]>-2<E[n]>.$$

2.8 设 E 是有限域 $k=\mathbb{F}_q$ 上的超奇异椭圆曲线，$t=q+1-|E(k)|=\pm 2\sqrt{q}$，则 $E(k)\simeq \mathbb{Z}_{\sqrt{q}\pm1}\times\mathbb{Z}_{\sqrt{q}\pm1}$.

2.9 设 E 是有限域 $k=\mathbb{F}_q$ 上的超奇异椭圆曲线，n 是 $E(k)$ 中任意一点的阶，则 $E[n]\subseteq E(\mathbb{F}_{q^c})$，其中 $c\leqslant 6$.

第 3 章　椭圆曲线离散对数问题

离散对数问题是许多公钥密码体制的基础. 设 G 为循环群, 其生成元为 α , 已知 $\beta \in G$, 求 k , 使得 $\beta = k\alpha$, 便是离散对数问题的一般表述形式. 若 $G = \mathbb{Z}_n, \alpha = 1$, 显然对于任意的 $\beta \in G$, 有 $k = \beta$, 即 $\mathbb{Z}_n$ 上的离散对数问题是容易的; 对于 $G = \mathbb{F}_p^{\times}$, 其上的离散对数问题已有亚指数时间的求解算法, 故而离散对数问题和 G 密切相关, 本章主要讨论椭圆曲线离散对数问题, 即已知有限域 $\mathbb{F}_q$ 上椭圆曲线 E , $P \in E(\mathbb{F}_q)$, P 的阶为 n , Q 属于 P 生成的循环群 (P) , 求 k 使得 $Q = kP$.

3.1 Shanks 的小步大步算法

Shanks 的小步大步算法 (baby-step giant-step algorithm) 的核心思想是测试 α 的倍数是否等于 β , 由于利用了某种数据结构, 故其优于强力搜索. 该算法[123] 于 1971 年由 Shanks 提出, 并计算了虚二次数域的类数, 其可以用于决定 Abel 群的结构.

该算法的基本思想为: 首先预计算并存储 α 的某些倍数 (小步, baby-steps) ; 然后对于某个整数 b , 计算 $\beta - b\alpha, \beta - 2b\alpha, \cdots$ (大步, giant-steps) , 直至 $\beta - ib\alpha$ 在预存储的表中出现, 则可以求得 β 相对于 α 的对数 $k = \log_{\alpha}\beta$, 即 $\beta = k\alpha$. 如果群中的每个元素有唯一的表示, 且对该表示可以排序, 那么可以利用二分查找, 使得其优于强力搜索. 虽然此限定限制了该算法的适用范围, 但大多数群均满足该限定条件.

阶为素数 p 的有限域的乘法群 $\mathbb{F}_p^{\times} = \{1, \cdots, p-1\}$, 其元素有唯一的有序表示; 而 $\mathbb{F}_{p^m}^{\times}$ 的每个元素可以表示为 $\mathbb{F}_p[X]$ 中次数小于 m 的多项式, 则首先以次数排序, 然后以系数排序, 故 $\mathbb{F}_{p^m}^{\times}$ 的元素也有唯一的有序表示; 对于 $\mathbb{F}_q$ 上的椭圆曲线 E , 因为其上的点均属于 $\mathbb{F}_q \times \mathbb{F}_q$, 故 E 的元素也有唯一的有序表示.

算法 3.1 (Shank 的小步大步算法)

输入　阶为 n 的群 G 的生成元 α , $\beta \in G$.

输出　$k = \log_{\alpha}\beta$.

(1) 确定小步的步数 b；

(2) 计算 $(i\alpha, i), 0 \leqslant i < b$，并将其依据第一分量排序存储；

(3) 大步的步数为 $g = \left\lceil \frac{n}{b} \right\rceil$；

(4) 计算 $\beta - jb\alpha, 0 \leqslant j < g$，并利用二分查找在预存储表中查找该值，若 $\beta - jb\alpha = i\alpha$，则 $k = i + jb$.

因为 $0 \leqslant k \leqslant n-1$，所以 k 有唯一的表示

$$k = jb + i, \qquad 0 \leqslant i < b, 0 \leqslant j < \left\lceil \frac{n}{b} \right\rceil,$$

即算法是正确的. 预存储表的计算与排序需要 $O(b\log b)$ 次操作，而第 (4) 步需要 $O(g\log b)$ 次操作，其中操作指群 G 中的加法或两个元素的比较. 已知 $gb = n$，可知当 $b = g = \lceil\sqrt{n}\rceil$ 时，$O((b+g)\log b)$ 取到最小值 $O(\sqrt{n}\log n)$，其存储空间为 $O(\sqrt{n}\log n)$.

Shanks 的小步大步算法还可以适用于 n 未知的情况. 若已知 n 的界，则可令 n 为该界来求解离散对数；若对 n 一无所知，则可选取随机数作为 n 运行该算法，如果没有求得离散对数，则重新选取随机数作为 n.

3.2 Pollard ρ 算法

当群的阶较大时，Shanks 的小步大步算法需要较大的存储空间. 1978 年，Pollard 提出了一个概率求解算法 [105]，其运算时间与小步大步算法相同，但不需要存储空间.

设 $G = T_1 \cup T_2 \cup T_3$，$T_1, T_2, T_3$ 是尺寸相同且互不相交的集合，随机选取 $a_0, b_0 \in \mathbb{Z}_n$，计算 $x_0 = a_0\alpha + b_0\beta$，并利用以下公式递归得到 $(x_i)_{i\geqslant 0}, (a_i)_{i\geqslant 0}, (b_i)_{i\geqslant 0}$：

$$x_{i+1} = \begin{cases} \beta + x_i, & x_i \in T_1 \\ 2x_i, & x_i \in T_2 \\ \alpha + x_i, & x_i \in T_3 \end{cases}$$

$$a_{i+1} = \begin{cases} a_i, & x_i \in T_1 \\ 2a_i, & x_i \in T_2 \\ a_i + 1, & x_i \in T_3 \end{cases}$$

$$b_{i+1} = \begin{cases} b_i + 1, & x_i \in T_1 \\ 2b_i, & x_i \in T_2 \\ b_i, & x_i \in T_3 \end{cases}$$

则 $x_i = a_i\alpha + b_i\beta, i \geqslant 0$. 因为 G 是有限群，所以序列 $(x_i)_{i\geqslant 0}$ 最终为周期序列，即存在唯一的最小整数 $\mu \geqslant 0$(称为预周期， preperiod) 和 $\lambda \geqslant 1$(称为周期，period)，使得 $x_1, \cdots, x_{\mu+\lambda-1}$ 互不相同且 $x_{i+\lambda} = x_i, i \geqslant \mu$. 将 x_i 作为平面上的点，则 $(x_i)_{i\geqslant 0}$ 在平面上所得的图恰好像希腊字母 ρ，故该算法称为 Pollard ρ 算法.

ρ 算法的目的是寻找 $i \neq j$, 使得 $x_i = x_j$，设 $\beta = k\alpha$，则

$$(a_i + kb_i)\alpha = a_i\alpha + b_i\beta = x_i = x_j = a_j\alpha + b_j\beta = (a_j + kb_j)\alpha,$$

故 $k(b_j - b_i) \equiv a_i - a_j \mod n$. 如果 $d = \gcd(n, b_j - b_i) = 1$，则可以精确求得 k；否则， k 有 d 个可能取值，当 d 较小时，可以直接通过判断 $k\alpha$ 是否等于 β 来求得正确的 k.

因为 $x_\mu = x_{\mu+\lambda}$ 是第一个匹配，所以为获得该匹配需要计算 $\mu + \lambda$ 个 x_i. 称映射

$$F : G \to G,$$
$$x \mapsto \begin{cases} \beta + x_i, & x_i \in T_1 \\ 2x_i, & x_i \in T_2 \\ \alpha + x_i, & x_i \in T_3 \end{cases}$$

为 Pollard 的插值函数. 若它是随机的，即是从 G 到 G 的所有映射中随机选取的，则由文献 [136] 知 $\mu + \lambda$ 的期望值近似为

$$\sqrt{\frac{\pi}{2}n} \approx 1.25\sqrt{n} \in O(\sqrt{n}).$$

对 Pollard 的插值函数随机性的分析请参看文献 [136]. 由于椭圆曲线中负点是容易计算的，所以可存储 $\pm F(Q)$ 中 Y 坐标作为整数值较小的点，则对于椭圆曲线群而言， $\mu + \lambda$ 的期望值近似为 $\sqrt{\pi n}/2$. 利用同样的方法，对于子域椭圆曲线，即椭圆曲线方程在基域 $\mathbb{F}_{p^{Bd}}$ 的子域 $\mathbb{F}_{p^d}$ 上,. Gallant,Lambert 和 Vanstone，

Wiener 和 Zuccherato 利用 Frobenius 映射将 $\mu+\lambda$ 的期望值减小为 $\sqrt{\pi n/B}/2$. 例如, 对 Koblitz 曲线, 求取 $E(\mathbb{F}_{2^m})$ 上的离散对数问题需要 $\sqrt{\pi n/m}/2$ 次点加.

Pollard 算法的存储空间依赖于匹配的寻找. 若同 Shanks 算法采用相同的数据结构,即按第一分量的大小将 (x_i, a_i, b_i) 排序存储,则为了找到一个匹配, Pollard 算法的存储空间为 $O(\sqrt{n})$.Pollard 建议采用 Floyd 提出的圈查找技术 [56](cycle finding technique) , 即计算 $(x_i, a_i, b_i, x_{2i}, a_{2i}, b_{2i})$, 直到 $x_i = x_{2i}$. 显然当 i 是 λ 的倍数且不小于 μ 时, $x_i = x_{2i}$. 因为 $x_{i+1} = F(x_i), x_{2(i+1)} = F(F(x_{2i}))$, 所以若使用该查找技术, 则不需要存储空间. 但寻找到第一个匹配的 i 的期望值大于 $\mu+\lambda$ 的期望值, 若 F 随机, 则为

$$\frac{\pi^2}{12}\sqrt{\frac{\pi}{2}n} \approx 1.03\sqrt{n}.$$

由于为了获得 $(x_i)_{i\geqslant 0}, (x_{2i})_{i\geqslant 0}$, 需要计算两次 $x_1, \cdots, x_i$, 所以 Pollard 算法要计算插值函数的次数平均为

$$3\frac{\pi^2}{12}\sqrt{\frac{\pi}{2}n} \approx 3.09\sqrt{n}.$$

文献 [12] 和 [114] 描述了高效的圈查找算法.

设 E 是定义在 $\mathbb{F}_q$ 上的椭圆曲线, $P \in E(\mathbb{F}_q)$ 的阶为素数 n,$Q \in (P)$. 文献 [136] 通过实验数据指出将椭圆曲线群分为 20 个互不相交的子群, 存储 8 个点, 且相邻点在 F 函数生成的序列中的下标间存在常数倍的关系, 则 ρ 算法的时间复杂度约为 $1.3\sqrt{n}$. 设 A 为黄金分割值 $\dfrac{\sqrt{5}-1}{2}$ 的精度为 $3+\lfloor\lg q\rfloor$(十进制) 的值, B 为大于 $2q^{1/4}$ 的最小素数, 则定义

$$\begin{aligned}
u_A^* : (P) &\to [0,1),\\
(x,y) &\mapsto Ay - \lfloor Ay\rfloor,\\
(0,1,0) &\mapsto 0;\\
u_B^* : (P) &\to [0,1),\\
(x,y) &\mapsto y/B - \lfloor y/B\rfloor,\\
(0,1,0) &\mapsto 0;\\
s : (P) &\to \{1,\cdots,20\},\\
Q &\mapsto \lfloor 20u^*(Q)\rfloor + 1,
\end{aligned}$$

其中，u^* 是 u_A^* 或 u_B^*. 设 m_i, n_i 均为 1 到 n 之间的随机数，令 $M_i = m_iP + n_iQ$，其中 $i = 1, \cdots, 20$ 为椭圆曲线上的随机点，则

$$F : (P) \to (P),$$
$$Q \mapsto Q + M_{s(Q)}.$$

在上述定义下，Teske 的 ρ 算法如下：

算法 3.2

输入 $\mathbb{F}_q$ 上椭圆曲线 E，$P \in E(\mathbb{F}_q)$ 的阶为素数 n，$Q \in (P)$.

输出 l 满足 $Q = lP$.

(1) 求取 $A(B)$；

(2) $\alpha \in_R [1, n], Y_0 = \alpha P, \alpha_0 = \alpha, \beta_0 = 0, c_0 = 0$；

(3) For $i = 1$ to 8: $Y_i = Y_0, \alpha_i = \alpha_0, \beta_i = \beta_0, c_i = 0$；

(4) For $i = 1$ to 20: $m_i, n_i \in_R [1, n], M_i = m_iP + n_iQ$；

(5) $i = 0, a_0 = \alpha_0, b_0 = 0, Z_0 = Y_0$；

(6) Do{

  $s = s(Z_i)$；

  $Z_i = Z_i + M_s, a_i = a_i + m_s, b_i = b_i + n_s$

  For $j = 1$ to 8: If $Z_i = Y_j$ break;

  If $i \geqslant 3c_1 - 1$

    For $j = 1$ to 7:$Y_j = Y_{j+1}, \alpha_j = \alpha_{j+1}, \beta_j = \beta_{j+1}, c_j = c_{j+1}$；

    $Y_8 = Z_i, \alpha_8 = a_i, \beta_8 = b_i$；

  $i++, c_8 = i$}

(7) 如果 $\gcd(b_i - \beta_j, n) = 1$，输出 $l = (\alpha_j - a_i)(b_i - \beta_j)^{-1} \mod n$；

(8) 否则返回第 (2) 步.

ρ 算法可以通过在不同的主机上采用不同的插值函数，即选取不同的 $\{(m_i, n_i)\}_{1 \leqslant i \leqslant 20}$，并将中间结果传送给服务器，由服务器在获得的元素中寻找匹配来实现并行化. 显然，如果将所有的中间结果均存储，则并行化所节省的运行时间会由查找所需的时间弥补，进而失去并行化的意义. 1999 年，Oorschot 等人 [103] 选择了一个特殊群元素 (distinguished group elements) 集合，如将二进制表示的高位为连续的 0 的元素作为特殊群元素，若插值计算所得的元素为特殊群元素，则将其发送给服务器，然后选择新的初始点再重复执行算法. 如果 ρ 算法在 m 个主机

上并行，则其运行时间大约为串行 ρ 算法的 $\dfrac{1}{m}$.

3.3 Pohlig-Hellman 算法

若群的阶 n 不是素数，则可以利用 n 的分解将 G 上的离散对数问题转换为 G 的 Sylow 子群 (阶为素数幂次的最大子群) 上的离散对数问题，而阶为素数幂次的群上的离散对数问题可通过阶为素数的群上的离散对数求解算法来获得，这便是 Pohlig-Hellman 算法的核心思想. 显然，若 p 是 n 的最大素因子，则 G 上离散对数问题的运行时间为 $O(\sqrt{p}\log p)$.

设 $n=\prod\limits_{i=1}^{l}p_i^{v_i}, k=\log_\alpha\beta$ ，若已知 $k \mod p_i^{v_i}$ ，则利用中国剩余定理便可求得 k. 设 $k\equiv\sum\limits_{i=0}^{v-1}b_ip^i \mod p^v$ ，因为 $\gamma=\dfrac{n}{p}\alpha$ 是 G 的阶为 p 的子群 G_p 的生成元，所以

$$\frac{n}{p}\beta=k\frac{n}{p}\alpha=k\gamma=b_0\gamma,$$

即 b_0 是 G_p 的离散对数值 $\log_\gamma\left(\dfrac{n}{p}\beta\right)$. 设 $b_0,\cdots,b_{j-1}$ 已经求得，定义 $k_j=\sum\limits_{i=0}^{j-1}b_ip^i$ ，则

$$\frac{n}{p^{j+1}}(\beta-k_j\alpha)=\left(\sum_{i=j}^{v-1}b_ip^{i-j}\right)\frac{n}{p}\alpha=b_j\gamma,$$

且 $b_j=\log_\gamma\left(\dfrac{n}{p^{j+1}}(\beta-k_j\alpha)\right)$ 是 G_p 上的离散对数值.

$\dfrac{n}{p^{j+1}}(\beta-k_j\alpha)$ 需要 $O(\log n)$ 次群的加法运算，而 G_p 上的离散对数求取需要 $O(\sqrt{p}\log p)$ 次加法运算，所以若 p 是 n 的最大素因子，令 $r=\sum\limits_{i=1}^{l}v_i$ ，则 $k \mod p_i^{v_i}, i=0,\cdots,l$ 的求取需要 $O(r(\log n+\sqrt{p}\log p))$ 次加法运算，利用中国剩余定理求取 k 需要 $O(r\log^2 n)$ 次比特运算，而群 G 的元素至少由 $\log n$ 比特表示，所以群的加法运算至少需要 $O(\log n)$ 次比特运算，故算法的时间复杂度为 $O(r(\log n+\sqrt{p}\log p))$ 次加法运算.

3.4 Index Calculus 算法

1997 年， Shoup[125] 证明了适用于任意 n 阶群的离散对数问题的求解算法需要 $O(\sqrt{p}\log p)$ 次群运算，其中 p 为 n 的最大素因子，而 Pohlig-Hellman 算法便是达到该时间复杂度的适用于任意群的算法，故仅可能对于特定的群，有更高效的离散对数求解算法. 本节将介绍有限域的乘法群 G 上离散对数问题的概率亚指数求解算法.

定义 3.4.1 输入尺寸为 $\log n$ 的 (非确定) 算法是亚指数的，如果存在常数 $c>0,\alpha\in(0,1)$ ，使得算法的 (期望) 运行时间为

$$L[\alpha,c]=O(e^{(c+o(1))(\log n)^{\alpha}(\log\log n)^{1-\alpha}}).$$

若 $\alpha=0$ ，则运行时间为 $L[0,c]$ 的算法为多项式时间算法；若 $\alpha=1$ ，则运行时间为 $L[1,c]$ 的算法为指数算法.

Index Calculus 算法由以下两部分组成.

(1) 收集线性等式　首先选定由 G 的某些元素组成的因子基 (factor base)$\Gamma=\{\gamma_1,\cdots,\gamma_t\}$ ，欲求得各 γ_i 的离散对数值. 重复选取随机数 $s\in\{0,\cdots,n-1\}$ ，计算 α^s ，并将其在 Γ 上分解，设

$$\alpha^s=\prod_{i=1}^{t}\gamma_i^{v_i},$$

则可得 $\mathbb{Z}_n$ 上的线性等式

$$s=\sum_{i=1}^{t}v_i\log_\alpha\gamma_i.$$

当线性等式的数量足够时，便可以唯一求得 $\log_\alpha\gamma_i, i=1,\cdots,t$.

(2) 求取对数值　随机选取整数 s 并在 Γ 上分解 $\beta\alpha^{-s}$ ，设

$$\beta\alpha^{-s}=\prod_{i=1}^{t}\gamma_i^{v_i},$$

则 $\log_\alpha\beta=s+\sum\limits_{i=1}^{t}v_i\log_\alpha\gamma_i$.

注意：当求取 G 上的多个离散对数值时，可以共用同一个因子基，而因子基越大，则收集线性等式越慢，求取对数值越快，故若在同一个群上欲求取的离散对数值多，则可以选取较大尺寸的因子基.

当 $G=\mathbb{F}_p^\times$ 时，取因子基 Γ 为小素数组成的集合，而 G 中的元素可以用 $\{0,\cdots,p-1\}$ 中的整数表示，故利用试除法便可以将 G 中的元素 γ 在 Γ 上分解. 若 $r\leqslant\log_2 p$ 是 γ 的所有素因子的个数，则至多经过 $t+r$ 次试除便可分解 γ 或证明 γ 无法在 Γ 上分解.

当 $G=\mathbb{F}_{p^m}$ 时，其元素可以用 $\mathbb{F}_p[X]$ 上次数小于 m 的多项式表示，取因子基 Γ 为次数较小的不可约多项式组成的集合，则对于 G 的元素 γ，至多利用 $m+t$ 次多项式除法便可将其分解或证明其在 Γ 上无法分解.

对上述算法已有许多改进. 1987 年， Pomerance[106] 给出了 $\mathbb{F}_p,\mathbb{F}_{2^m}$ 上运行时间为 $L[1/2,\sqrt{2}]$ 的离散对数求取算法，这是目前对运行时间给出证明的最高效算法； 1984 年， Coppersmith[20] 给出了运行时间为 $L[1/3,c]$ 的 $\mathbb{F}_{2^m}$ 上离散对数求解算法，其中 c 约为 1.4； 1993 年， Gordon 基于数域筛法 (number field sieve) 提出了运行时间为 $L[1/3,4/\sqrt[3]{9}]$ 的 $\mathbb{F}_p$ 上离散对数求解算法. 后两个算法的运行时间均没有给出严格证明.

3.5 椭圆曲线离散对数问题

由于对于一般的椭圆曲线群，无法选取合适的因子基，故 Index Calculus 算法不能用来求解一般椭圆曲线群上的离散对数问题 (Index Calculs 算法在椭圆曲线群上的分析可以参看文献 [92],[129])，而已有的求解算法均为指数时间的. 但是对于一些特殊的椭圆曲线群，如超奇异椭圆曲线、阶为 p 的椭圆曲线等，其上离散对数问题有高效的求解算法. 以下将分别对其做介绍.

3.5.1 MOV 算法

MOV 算法 [86] 是 Menezes 、 Okamoto 和 Vanstone 于 1993 年提出的，其核心思想是将椭圆曲线离散对数问题转化为某个有限域的乘法群上的离散对数问题. 特别地，对于超奇异椭圆曲线，该转化导致了亚指数的 ECDLP 求解算法.

设 $\mathbb{F}_q$ 的特征为 p， E 为其上的椭圆曲线， $P\in E(\mathbb{F}_q)$ 的阶为奇素数 n， $R=lP$，欲求取 l.

因为 $E(\mathbb{F}_{q^k})\simeq\mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2},n_1|q^k-1$，而 $E[n]\simeq\mathbb{Z}_n\times\mathbb{Z}_n$ 是 $E(\mathbb{F}_{q^k})$ 的子群，由下述命题知 $n|n_1$，所以 $n|q^k-1$，即 $n|q^k-1$ 是将椭圆曲线离散对数问题利用 MOV 约化到 $\mathbb{F}_{q^k}$ 上的必要条件.

命题 3.5.1 设 G 是有限 Abel 群, $G \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}, n_1, n_2 \geqslant 1, n_1|n_2$, H 是 G 的子群, 则

$$H \simeq \mathbb{Z}_{m_1} \times \mathbb{Z}_{m_2}, m_1, m_2 \geqslant 1, m_1|m_2, m_1|n_1, m_2|n_2.$$

证明 令 $G[n]$ 为 G 中 n 阶元构成的子群,

$$G[n^\infty] = \cup_{i=0}^{\infty} G[n^i].$$

则对于 $|G|$ 的素因子 p , $G[p^\infty]$ 是 G 的 p-Sylow 子群, 即阶为 p 的幂次的最大子群, 递归应用引理 2.5.13 得

$$G \simeq \times_{p||G|} G[p^\infty] \simeq \times_{p||G|} (\mathbb{Z}_{p^{v_1}} \times \mathbb{Z}_{p^{v_2}}).$$

其中, v_i 为 p 在 n_i 中的指数, 故只需证结论对于 p-Sylow 子群成立, 然后利用中国剩余定理便可知结论对于 G 成立. 以下设

$$G \simeq \mathbb{Z}_{p^{v_1}} \times \mathbb{Z}_{p^{v_2}}, 0 \leqslant v_1 \leqslant v_2.$$

若 G 是循环群, 即 $v_1 = 0$, 由循环群的子群为循环群且 $|H|||G|$ 知结论成立; 否则, 由 $|H|||G|$ 和定理 2.5.11 得

$$H \simeq \mathbb{Z}_{p^{\mu_1}} \times \cdots \times \mathbb{Z}_{p^{\mu_1}}, 1 \leqslant \mu_1 \leqslant \cdots \leqslant \mu_s,$$

因为

$$G[p] \simeq p^{v_1-1}\mathbb{Z}_{p^{v_1}} \times p^{v_2-1}\mathbb{Z}_{p^{v_2}} \simeq \mathbb{Z}_p \times \mathbb{Z}_p,$$

所以 $|G[p]| = p^2$, 进而 $|H[p]| = p^s$, 而 $H[p] \subseteq G[p]$, 故 $s \leqslant 2$; 已知 p^{v_2}, p^{μ_2} 分别是 G, H 中元素的最大阶, 显然有 $\mu_2 \leqslant v_2$, 若 $\mu_1 > v_1$, 则 $v_2 \geqslant \mu_2 \geqslant \mu_1 > v_1$,

$$|G[p^{\mu_1}]| = p^{v_1}p^{\mu_1} < p^{\mu_1}p^{\mu_1} = |H[p^{\mu_1}]|,$$

矛盾, 故 $\mu_1 \leqslant v_1$. 结论得证.

实际上, 若 $p \nmid n, n \nmid q-1$, 则 $E[n] \subseteq E(\mathbb{F}_{q^k})$ 当且仅当 $n|q^k - 1$[86].

引理 3.5.2 设 $E[n] \subseteq E(\mathbb{F}_q)$, n 和 q 互素, $P \in E[n]$ 的阶为 n , 则对于任意的 $P_1, P_2 \in E[n]$, $P_1 - P_2 \in (P)$ 当且仅当 $e_n(P, P_1) = e_n(P, P_2)$.

证明 已知 $P_1 = P_2 + kP$ ，则显然有

$$
\begin{aligned}
e_n(P, P_1) &= e_n(P, P_2)e_n(P, P)^k \\
&= e_n(P, P_2).
\end{aligned}
$$

已知 $e_n(P, P_1) = e_n(P, P_2)$ ，若 $P_1 - P_2 \notin (P)$ ，设 P, Q 为 $E[n] \cong \mathbb{Z}_n \times \mathbb{Z}_n$ 的生成元，则存在 a_1, a_2, 使得 $P_1 - P_2 = a_1P + a_2Q, a_2Q \neq O, e_n(P, a_2Q) = 1$. 对于 $E[n]$ 中的任意点 $b_1P + b_2Q$ ，有

$$
\begin{aligned}
e_n(a_2Q, b_1P + b_2Q) &= e_n(a_2Q, P)^{b_1} e_n(Q, Q)^{a_2b_2} \\
&= e_n(P, a_2Q)^{-b_1} = 1.
\end{aligned}
$$

因为 Weil 对 e_n 具有非退化性，所以 $a_2Q = O$ ，矛盾. 即 $P_1 - P_2 \in (P)$. 结论证毕.

定理 3.5.3 *存在 $Q \in E[n]$ 使得 $e_n(P, Q)$ 为 n 次本原单位根.*

证明 对于任意的点 $Q \in E[n]$ ，有 $e_n(P, Q)$ 为 n 次单位根. 又因为在 $E[n]$ 中有 n 个 (P) 的陪集，且上述引理说明在 P 固定的条件下，不同的陪集代表元 Q 对应的 Weil 对 $e_n(P, Q)$ 是不同的 n 次单位根，所以结论显然成立.

设 $N \in \mathbb{Z}$ ，若 $n^r | N$ 且 $n^{r+1} \nmid N$ ，则记 $n^r || N$. 对于一般椭圆曲线，即不限定其是超奇异的，有如下的 MOV 约化算法.

算法 3.3 (MOV 算法)

输入 $\mathbb{F}_q, E, P, n, R$;

输出 $l, R = lP$.

(1) 确定满足 $E[n] \subseteq E(\mathbb{F}_{q^k})$ 的最小整数，记作 k ；

(2) 求取 $E(\mathbb{F}_q)$ 的阶，记作 N_1 ， $r \in \mathbb{Z}$ 满足 $n^r || N_1$ ；

(3) 求取 $E(\mathbb{F}_{q^k})$ 的阶，记作 N_k ；

(4) $d \in \mathbb{Z}$ 满足 $n^d || N_k$ ，令 $s = d - r$ ；

(5) 若 $r \leqslant s$:

① $Q \in_R E(\mathbb{F}_{q^k})$ ；

② $Q' = \frac{N_k}{n^{r+1}} Q \in E[n]$ ；

③ $\alpha = e_n(P, Q')$ ，若 $\alpha = 1$ ， Goto ①;

(6) 若 $r > s$:

① $Q \in_R E(\mathbb{F}_{q^k})$ ；

② $Q' = (\phi - 1)(\frac{N_k}{n^{r+1}}Q) \in E[n]$，若 $Q' = O$， Goto ①；

③ $\alpha = e_n(P, Q')$；

(7) 计算 $\beta = e_n(R, Q')$；

(8) 在 $\mathbb{F}_{q^k}$ 中求取 $l = \log_\alpha \beta$，并输出 l.

ϕ 表示 E 上的 Frobenius 映射. 因为 $\beta = e_n(lP, Q') = e_n(P, Q')^l = \alpha^l$，所以算法输出正确. 文献 [124] 证明了上述算法中第 (5) 步的③中 $\alpha = 1$ 的概率为 $1/n$，当 n 为大素数时，该算法成功的概率几乎为 1. 因为 Weil 对是概率多项式时间可计算的 [84]，故算法是有效的.

为了方便计算，本节还给出 Weil 对的一个等价定义，其相关证明请读者作为习题. 设除子 $D = \sum\limits_{P\in E} n_P < P >$，其支撑 $\mathrm{Supp}(D) = \{P \in E : n_P \neq 0\}$，$f \in K(E)$ 且 $\mathrm{div}(f)$ 和 D 的支撑互不相交，则定义

$$f(D) = \prod_{P\in \mathrm{Supp}(D)} f(P)^{n_P}.$$

定理 3.5.4 令 $f, g \in K(E)$ 使得 $\mathrm{div}(f)$ 和 $\mathrm{div}(g)$ 的支撑互不相交，则

$$f(\mathrm{div}(g)) = g(\mathrm{div}(f)).$$

对于 m 扭点 S, T，令

$$D_S \sim < 2S > - < S >,$$

$$D_T \sim < 2T > - < T >,$$

且 D_S, D_T 无相同的支撑点,则存在 $f_S, f_T \in K(E)$,使得 $\mathrm{div}(f_S) = mD_S, \mathrm{div}(f_T) = mD_T$.

定理 3.5.5 对于 m 扭点 S, T，有 $e_m(S, T) = \dfrac{f_S(D_T)}{f_T(D_S)}$.

下面仅给出 Weil 对的求取过程，证明请见文献 [84].

设 D 是零次除子，且 $kP, 0 \leqslant k < n$ 均不属于 D 的支撑，定义

$$U = \{kP : 0 \leqslant k < n\} \times \bar{\mathbb{F}}_q^{\times},$$

其上的加法 $\oplus$ 为

$$(k_1P, c_1) \oplus (k_2P, c_2) = ((k_1 + k_2)P, c_1c_2h(D)),$$

$$h = \frac{l_{k_1P,k_2P}}{v_{(k_1+k_2)P}},$$

其中， l_{k_1P,k_2P} 为 k_1P,k_2P 所决定的直线， $v_{(k_1+k_2)P}$ 为过 $(k_1+k_2)P$ 的垂线，则 $(U,\oplus)$ 为群 (见习题 3.3).$k\odot(P,1)$ 表示 k 个 $(P,1)$ 进行 $\oplus$ 运算，则 $k\odot(P,1)=(kP,g_k(D))$ ，其中

$$\mathrm{div}(g_k)=k<P>-<kP>-(k-1)<O>.$$

令

$$\begin{aligned}D_Q=<2Q>-<Q> \quad &, \quad D_P=<2P>-<P>,\\ \mathrm{div}(f_Q)=nD_Q \quad &, \quad \mathrm{div}(f_P)=nD_P,\\ \mathrm{div}(\hat{f}_Q)=n<Q>-n<O> \quad &, \quad \mathrm{div}(\hat{f}_P)=n<P>-n<O>,\end{aligned}$$

则 $n\odot(P,1)=(O,\hat{f}_P(D_Q))$ ，若计算中途失败，则 $Q\in(P)$. 又因为

$$\mathrm{div}\left(\frac{f_Q}{\hat{f}_Q}\right)=\left(\frac{v_{2Q}}{l_{Q,Q}}\right)^n=g_Q^n,$$

则由定理 3.5.5 知

$$e_n(Q,P)=\frac{f_Q(D_P)}{f_P(D_Q)}=\frac{\hat{f}_Q(D_P)g_Q(D_P)^n}{\hat{f}_P(D_Q)g_P(D_Q)^n}.$$

算法 3.4

输入 椭圆曲线点 P ，正整数 k ，零次除子 D.

输出 $(0,(Q,c)=k\odot(P,1))$ 或 $(i,Q,0)$.

(1) $k=\sum\limits_{i=0}^{t}a_i2^i, a_i\in\{0,1\}, c=1, Q=O, b=0$;

(2) For $i=t$ to 0

如果 $a_i=1$:$h=\dfrac{l_{Q,P}}{v_{Q+P}}$,

若 D 的支撑中有点 $Q,P,P+Q,O$ ，则中止，并输出 $(b,Q,0)$;

否则 $b++, c=ch(D), Q=Q+P$;

$h=\dfrac{l_{Q,Q}}{v_{2Q}}$,

若 D 的支撑中有点 $Q,2Q,O$ ，则中止，并输出 $(b,Q,0)$;

否则 $b=2b, c=ch(D), Q=2Q$;

(3) 输出 $(0,Q,c)$.

算法 3.5

输入 椭圆曲线点 P, Q, 正整数 n.

输出 (True,Weil 对 $e_n(Q,P)$) 或 (False, $\log_Q P$).

(1) 令 $D_Q =< 2Q > - < Q >$;

(2) 令 $D_P =< 2P > - < P >$;

(3) $(b,R,c) =$ 算法 3.4(n,P,D_Q) ，若 $c=0$ ，存在 $i \in \{b, 2b, b+1, 1, b/2, (b+1)/2\}$ 使得 $Q = iP$ ，则输出 (False,i^{-1} mod ord(Q)),ord(Q) 为 Q 的阶;

(4) (b,S,d) = 算法 3.4(n,Q,D_P) ，若 $d = 0$ ，存在 $i \in \{b, 2b, b+1, 1, b/2, (b+1)/2\}$ 使得 $P = iQ$ ，则输出 (False, i) ;

(5) $g = v_{2Q}/l_{Q,Q}(D_P), h = v_{2P}/l_{P,P}(D_Q)$;

(6) 输出 $\left(\text{True}, c = \dfrac{dg^n}{ch^n}\right)$.

对于超奇异椭圆曲线 E ，即 $|E(\mathbb{F}_q)| \equiv 1 \mod p$. 设 $E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}, n_1|n_2$ ，则 $E(\mathbb{F}_{q^k}) \simeq \mathbb{Z}_{cn_2} \times \mathbb{Z}_{cn_2}$ ，其中 k 为满足 $E[n_2] \subseteq E(\mathbb{F}_{q^k})$ 的最小整数. 表 3.1 给出了其结构 (见习题 3.5).

表 3.1 超奇异椭圆曲线的结构

$t = q+1-\|E(\mathbb{F}_q)\|$	群结构	n_2	k	c
0	循环	$q+1$	2	1
0	$\mathbb{Z}_2 \times \mathbb{Z}_{\frac{q+1}{2}}$	$\dfrac{q+1}{2}$	2	2
$\pm\sqrt{q}$	循环	$q+1\mp\sqrt{q}$	3	$\sqrt{q}\pm 1$
$\pm\sqrt{2q}$	循环	$q+1\mp\sqrt{2q}$	4	$q\pm\sqrt{2q}+1$
$\pm\sqrt{3q}$	循环	$q+1\mp\sqrt{3q}$	6	$\dfrac{q+1}{q+1\pm\sqrt{3q}}$
$\pm 2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}\mp 1} \times \mathbb{Z}_{\sqrt{q}\mp 1}$	$\sqrt{q}\mp 1$	1	1

所以对于超奇异椭圆曲线，点 Q 的选取更加简单，从而得到如下针对超奇异椭圆曲线的 MOV 算法:

(1) 随机选取 $Q' \in E(\mathbb{F}_{q^k})$ ，令 $Q = \dfrac{cn_2}{n} Q'$ ，计算 $\alpha = e_n(P,Q)$;

(2) 计算 $\beta = e_n(R,Q)$;

(3) 在 $\mathbb{F}_{q^k}$ 上求取 $l' = \log_\alpha \beta$;

(4) 若 $l'P = R$ ，则 $l = l'$ ；否则 α 不是 n 次本原单位根，返回第 (1) 步.

1994 年， Frey 和 Rück[36] 利用 Tate 对给出了与 MOV 约化算法相类似的约化算法，其也是将椭圆曲线离散对数问题转化为 $\mathbb{F}_{q^k}$ 的乘法群上，且 $n|q^k-1$ 是约化到 $\mathbb{F}_{q^k}$ 的充要条件. 以下对其做简单介绍. 设 E 是 $\mathbb{F}_q$ 上的椭圆曲线，若

素数 $n|q^k-1$ ，令 $\mathbb{K}=\mathbb{F}_{q^k}$ ，则

$$t_n: E(\mathbb{K})[n]\times E(\mathbb{K})/nE(\mathbb{K})\to \mathbb{K}^*/(\mathbb{K}^*)^n$$
$$(A,B)\mapsto f_A(D_B)$$

是非退化双线性映射，称为 Tate 对，其中 D_A 是与 $<A>-<O>$ 等价的除子， $\mathrm{div}(f_A)=nD_A$ ， D_B 是与 $<B>-<O>$ 等价的除子，且 D_A,D_B 的支撑互不相交. 若 P 是 n 阶点，则存在 $Q\in E(\mathbb{K})/nE(\mathbb{K})$ 满足 $t_n(P,Q)^{\frac{q^k-1}{n}}$ 为 n 次本原单位根 μ_n ，故

$$(P)\to(\mu_n),$$
$$S\mapsto t_n(S,Q)^{\frac{q^k-1}{n}}$$

为同构映射. FR 约化算法如下.

算法 3.6

输入 $\mathbb{F}_q$ 上椭圆曲线 E ， $P\in E(\mathbb{F}_q)$ 的阶为素数 n,$R\in(P)$.

输出 l 满足 $R=lP$.

(1) 求最小正整数 k 满足 $n|q^k-1$ ，令 $\mathbb{K}=\mathbb{F}_{q^k}$ ；

(2) $S,T\in_R E(\mathbb{K})$ ；

(3) 求 $f\in\mathbb{K}(E)$ 满足 $\mathrm{div}(f)=n(<P>-<O>)$ ，求 $\alpha=f(S)/f(T)$ ；

(4) 求 $\gamma=\alpha^{\frac{q^k-1}{n}}$ ，若 $\gamma=1$ ，则返回第 (2) 步；

(5) 求 $g\in\mathbb{K}(E)$ ，满足 $\mathrm{div}(g)=n(<R>-<O>)$ ，求 $\beta=g(S)/g(T),\delta=\beta^{\frac{q^k-1}{n}}$ ；

(6) 在 $\mathbb{K}$ 中求取 $\log_\gamma\delta$.

MOV 约化比 FR 约化要多计算一次 $n\odot(P,1)$ ，且 FR 约化适用于 $n|q^k-1$ ，其中 k 较小的条件，而 MOV 约化只能适用于 $n|q^k-1,k>1$ 较小的条件，这里的 n 均为与特征 p 互素的素数，故可以认为 FR 约化优于 MOV 约化.

由于上述约化算法的存在，为保证椭圆曲线密码体制安全，必须要求对于满足 $n|q^k-1$ 的最小的 k ，有 $\mathbb{F}_{q^k}^\times$ 上离散对数问题不可解. 若 q 的比特尺寸大于 160 ，则可以要求 $k\geqslant 20$.

3.5.2 阶为 p的椭圆曲线

对于阶为 p 的椭圆曲线上的离散对数问题，有非常高效的求解算法，其核心思想是将问题转化为加法群 $\mathbb{F}_p=\{0,\cdots,p-1\}$ 上的离散对数问题.

设 $q=p^n, p\neq 2,3$ 为素数， K 为 $\mathbb{F}_p$ 的代数闭域， $E: Y^2=X^3+aX+b$ 是 $\mathbb{F}_q$ 上的椭圆曲线且 $p||E(\mathbb{F}_q)|$ ， $P\in E(\mathbb{F}_q)$ 为 p 阶点，则任意的 $Q\in(P)$ ，有 $p(<Q>-<O>)$ 是主除子，故存在 $f_Q\in\mathbb{F}_q(E)$, 使得 $\mathrm{div}(f_Q)=p(<Q>-<O>)$.

定理 3.5.6 设 $f\in K(E), \mathrm{div}(f)=pD, D$ 不是主除子，令 $f'=\dfrac{Df}{DX}$ ，则 $\mathrm{div}(f')=\mathrm{div}(f)-\mathrm{div}(Y)$.

证明 设 $D=\sum\limits_{Q\in E} n_Q<Q>$ ， $f=t_Q^{pn_Q}f_1$ ，其中 $\mathrm{ord}_Q(f_1)=0$ ， t_Q 为 Q 点的一致性参数，

$$t_Q=\begin{cases}\dfrac{X}{Y}, & 若Q=O\\ X-a, & 若Q=(a,b)不是二阶点\\ Y, & 若Q=(a,0)是二阶点\end{cases}$$

(1) 若 $Q\neq O$ 不是二阶点，则 $\dfrac{Df}{DX}=\dfrac{t_Q^{pn_Q}Df_1}{DX}$ ，故 $\mathrm{ord}_Q\left(\dfrac{Df}{DX}\right)=pn_Q+m_Q$ ，其中 $m_Q=\mathrm{ord}_Q\left(\dfrac{Df_1}{DX}\right)\geqslant 0$;

(2) 若 Q 是二阶点，则

$$\begin{aligned}\frac{Df}{DX}&=\frac{Df}{DY}\cdot\frac{DY}{DX}\\&=\frac{Y^{pn_Q}Df_1}{DY}\cdot\frac{DY}{DX}\\&=Y^{pn_Q}\cdot\frac{3X^2+a}{2Y}\cdot\frac{Df_1}{DY},\end{aligned}$$

故 $\mathrm{ord}_Q\left(\dfrac{Df}{DX}\right)=pn_Q-1+m_Q$ ，其中 $m_Q=\mathrm{ord}_Q\left(\dfrac{Df_1}{DY}\right)\geqslant 0$;

(3) 若 $Q=O$ ，则

$$\begin{aligned}\frac{Df}{DX}&=\frac{Df}{Dt_Q}\cdot\frac{Dt_Q}{DX}\\&=t_Q^{pn_Q}\cdot\frac{Df_1}{Dt_Q}\cdot\frac{Dt_Q}{DX},\end{aligned}$$

$$\begin{aligned}\frac{Dt_Q}{DX}&=\frac{D\frac{X}{Y}}{DX}\\&=\frac{YDX-XDY}{Y^2DX}\end{aligned}$$

$$= \frac{Y - X\frac{3X^2+a}{2Y}}{Y^2}$$
$$= \frac{2Y^2 - (3X^2+a)X}{2Y^3}$$
$$= \frac{-X^3 + aX + 2b}{2Y^3},$$

故 $\mathrm{ord}_Q\left(\frac{Df}{DX}\right) = pn_Q + 3 + m_Q$ ，其中 $m_Q = \mathrm{ord}_Q\left(\frac{Df_1}{Dt_Q}\right) \geqslant 0$.

设 P_1, P_2, P_3 为 E 的三个二阶点，则

$$\begin{aligned}\mathrm{div}(f') &= \sum_{Q\in E} \mathrm{ord}_Q(f') < Q > \\ &= \sum_{Q\in E} pn_Q < Q > + \sum_{Q\in E} m_Q < Q > - < P_1 > - < P_2 > - < P_3 > + 3 < O > \\ &= \mathrm{div}(f) + \sum_{Q\in E} m_Q < Q > - \mathrm{div}(Y).\end{aligned}$$

因为对于任意的 $Q \in E$ 有 $m_Q \geqslant 0$ 且 $\sum\limits_{Q\in E} m_Q < Q >$ 为主除子，所以对于任意的 $Q \in E$ 有 $m_Q = 0$. 结论得证.

定理 3.5.7 下述映射为 (P) 到加法群 $\mathbb{F}_q(E)$ 的单同态：

$$\phi : (P) \to \mathbb{F}_q(E),$$
$$Q \mapsto \frac{f'_Q}{f_Q}.$$

证明 设 D'_Q 和 D_Q 等价，则存在有理函数 g ，使得 $\mathrm{div}(g) = D_Q - D'_Q$. 设有理函数 f 满足 $\mathrm{div}(f) = pD'_Q$ ，则 $f_Q = cg^p f$ ，其中 $c \in \mathbb{F}_q^\times$ ，

$$\frac{f'_Q}{f_Q} = \frac{(cg^p f)'}{cg^p f} = p\frac{g' g^{p-1} f}{g^p f} + \frac{g^p f'}{g^p f} = \frac{f'}{f},$$

所以该映射是定义好的.

若 $f'_Q = 0$ ，则存在有理函数 f 使得 $f_Q = f(X,Y)^p$ ，故 D_Q 为主除子，即 $Q = O$ ，亦即 ϕ 为单映射.

设 $Q_1, Q_2 \in (P)$ ，可令 $D_{Q_1+Q_2} = D_{Q_1} + D_{Q_2}$ ，则 $f_{Q_1+Q_2} = cf_{Q_1} f_{Q_2}$ ，其中 $c \in \mathbb{F}_q^\times$ ，有

$$\frac{f'_{Q_1+Q_2}}{f_{Q_1+Q_2}} = \frac{(f_{Q_1} f_{Q_2})'}{f_{Q_1} f_{Q_2}} = \frac{f'_{Q_1} f_{Q_2}}{f_{Q_1} f_{Q_2}} + \frac{f_{Q_1} f'_{Q_2}}{f_{Q_1} f_{Q_2}} = \frac{f'_{Q_1}}{f_{Q_1}} + \frac{f'_{Q_2}}{f_{Q_2}},$$

所以 ϕ 是同态. 结论证毕.

推论 3.5.8 设 $R \in (P) \setminus \{O\}$ 满足对于任意的 $Q \in (P)$ ，R 均不属于 D_Q 的支撑，则

$$\psi : (P) \to \mathbb{F}_q,$$
$$Q \mapsto \frac{f_Q'}{f_Q}(R)$$

是 (P) 到加法群 $\mathbb{F}_q$ 的单同态.

证明 若 $\psi(Q) = 0$ ，则 R 是 $\frac{f_Q'}{f_Q}$ 的零点，又因为 $R \in (P)$ ，所以 R 不是二阶点，故 D_Q 为主除子，即 $Q = O$ ，所以 ψ 是单映射. 由定理易知 ψ 是同态. 结论证毕.

由该推论即可将 $E(\mathbb{F}_q)$ 上的离散对数问题转化为 $\mathbb{F}_q$ 上的离散对数问题，算法描述如下.

算法 3.7

输入 素数 $p > 3$ ，$\mathbb{F}_q$ 上椭圆曲线 E ，$p||E(\mathbb{F}_q)|$ ，p 阶点 $P, Q \in (P)$.

输出 l 满足 $Q = lP$.

(1) $p = \sum_{i=1}^{t} a_i 2^i, a_i = 0, 1$ ；

(2) 选取 $R \in (P) \setminus \{O\}$ 使得 R 不属于

$$\pm \left(\sum_{i=j}^{t} a_i 2^{i-j} \right) P, \pm \left(2 \sum_{i=j}^{t} a_i 2^{i-j} \right) P, \pm \left(\sum_{i=j}^{t} a_i 2^{i-j} \right) Q, \pm \left(2 \sum_{i=j}^{t} a_i 2^{i-j} \right) Q,$$

其中 $j = 1, \cdots, t$ ；

(3) 求取 $b_1 = \frac{f_Q'}{f_Q}(R)$ ；

(4) 求取 $b_2 = \frac{f_P'}{f_P}(R)$ ；

(5) 输出 $l = b_1 b_2^{-1} \mod p$.

上述算法中还遗留了一个问题，即 $\frac{f_Q'}{f_Q}(R), \frac{f_P'}{f_P}(R)$ 的求取. 对于集合 $U = (P) \times \mathbb{F}_q^+$ 定义 $\oplus$:

$$(k_1 P, c_1) \oplus (k_2 P, c_2) = \left((k_1 + k_2) P, c_1 + c_2 + \frac{h'}{h}(R) \right),$$

其中， $h=\dfrac{l_{k_1P,k_2P}}{v_{(k_1+k_2)P}}$ ，可以证明 $(U,\oplus)$ 为群.

定理 3.5.9 令 $k\odot(P,0)$ 表示 k 个 $(P,0)$ 进行 $\oplus$ 运算，则 $k\odot(P,0)=\left(kP,\dfrac{g_k'}{g_k}(R)\right)$ ，其中有理函数 g_k 满足 $\mathrm{div}(g_k)=k<P>-<kP>-(k-1)<O>$.

证明 当 $k=0,1$ 时，结论显然成立. 设小于 k 时结论均成立，下证等于 k 时结论也成立. 设 $k=k_1+k_2,k_1,k_2\geqslant 1$ ，则

$$
\begin{aligned}
k\odot(P,0)&=(k_1\odot(P,0))\oplus(k_2\odot(P,0))\\
&=\left(k_1P,\frac{g_{k_1}'}{g_{k_1}}(R)\right)\oplus\left(k_2P,\frac{g_{k_2}'}{g_{k_2}}(R)\right)\\
&=\left(kP,\frac{g_{k_1}'}{g_{k_1}}(R)+\frac{g_{k_2}'}{g_{k_2}}(R)+\frac{l_{k_1P,k_2P}'}{l_{k_1P,k_2P}}(R)-\frac{v_{kP}'}{v_{kP}}(R)\right)\\
&=\left(kP,\frac{f'}{f}(R)\right).
\end{aligned}
$$

其中， $f=g_{k_1}g_{k_2}l_{k_1P,k_2P}v_{kP}^{-1}$ ，则

$$
\begin{aligned}
\mathrm{div}(f)&=\mathrm{div}(g_{k_1})+\mathrm{div}(g_{k_2})+\mathrm{div}(l_{k_1P,k_2P})-\mathrm{div}(v_{kP})\\
&=k<P>-<kP>-(k-1)<O>\\
&=\mathrm{div}(g_k).
\end{aligned}
$$

结论证毕.

令 $c_k=\dfrac{g_k'}{g_k}(R)$. 因为 P 是 p 阶点，所以 $\mathrm{div}(g_p)=p<P>-p<O>=\mathrm{div}(f_P)$ ，即

$$
p\odot(P,0)=\left(O,\frac{f_P'}{f_P}(R)\right).
$$

以上说明利用该定理在初始值为 $c_0=0,c_1=0$ 下类似于 Shamir 算法即可求得 c_p ，其所需时间为 $O(\log_2 p)$ 次有限域的乘法. 算法第 (2) 步中 R 的选取确保了可以按上述方法顺利求得 c_p ，而 (P) 中至多有 $8t\leqslant 8\log_2 p$ 个点不能选取. 当 $p\geqslant 40$ 时， (P) 中一定有满足条件的 R. 随机选取的 R 满足条件的概率不小于 $1-8\dfrac{\log_2 p}{p}$ ，所以当 p 为大素数时，随机选取的点为 R 的概率近似为 1. 若要确保 R 以概率 1 选取，则可预先进行 $8\log_2 p$ 次标量乘法，将不满足条件的点排除，其复杂度为 $2\log_2 p$ 次点加和 $2\log_2 p$ 次倍点.

3.6 椭圆曲线公钥密码

自从 1976 年 Diffie 和 Hellman 提出了公钥密码之后，各种公钥密码体制纷纷出台，它们几乎均是基于某个数学难题的，而其中大数分解问题和离散对数问题是公钥密码最核心的两个难题. 目前，大数分解问题和有限域的乘法群上的离散对数问题已有亚指数时间的求解算法，故而为保证实际的安全，基于这些问题的公钥密码的密钥尺寸必须大于 1000 比特，这在一定程度上限制了这些密码在资源受限环境下的使用.

1985 年， Neal Koblitz 和 Victor Miller 各自独立地提出了椭圆曲线公钥密码，其安全性是基于椭圆曲线离散对数问题的. 由于一般椭圆曲线群上的离散对数问题还没有亚指数时间的求解算法，所以椭圆曲线公钥密码体制有着其他公钥密码体制所无法比拟的优点，如在相同的安全强度下，密钥尺寸比较小，选择余地比较大等，这使得椭圆曲线公钥密码可以适用于各种受限环境. 本节仅介绍一些简单的椭圆曲线公钥密码体制.

3.6.1 安全参数的选取

椭圆曲线密码体制的系统参数为 $D=(q,a,b,G,n,h)$ ：

(1) 特征为 p 的有限域 $\mathbb{F}_q$ ；

(2) 参数 a 和 b ，定义 $\mathbb{F}_q$ 上椭圆曲线 E ，即 $Y^2=X^3+aX+b(p>3)$ 或 $Y^2+XY=X^3+aX^2+b(p=2)$ ；

(3) 作为基点的阶为 n 的椭圆曲线上点 G ；

(4) 余因子 h ，等于椭圆曲线的阶除以 n 而得到的因子.

从实现和安全角度考虑，主要为抵抗上述的 ECDLP 求解算法，因此必须对这些参数作特殊的限制：

(1) $q=p$ 或 $q=2^m$ ，其中 m 是素数;

(2) 椭圆曲线是非超奇异的 (Non-supersingular) ；

(3) 基点的阶 n 不整除 $q^k-1(1\leqslant k\leqslant c)$ ，实际中常取 c 为 20 ；

(4) 椭圆曲线是非异常的 (Non-anomalous) ，即 $|E(\mathbb{F}_q)|\neq q$.

满足上述条件的系统参数称为一般参数.

例 3.1

$$
\begin{aligned}
q &= p \\
&= 6277101735386680763835789423207666416083908700390324961279192\text{bits}, \\
n &= 6277101735386680763835789423176059013767194773182842284081, \\
h &= 1, \\
a &= -3, \\
b &= 0x64210519e59c80e70fa7e9ab72243049feb8deecc146b9b1, \\
G &= (x, y), \\
x &= 0x188da80eb03090f67cbf20eb43a18800f4ff0afd82ff1012, \\
y &= 0x07192b95ffc8da78631011ed6b24cdd573f977a11e794811.
\end{aligned}
$$

上述例子是 NIST 所建议使用的一个椭圆曲线参数，其满足一般参数的条件，故是一般参数. NIST 建议的所有参数可以参阅 NIST 所写的 “ Recommended elliptic curves for federal government”.

一般参数上 ECDLP 求解的最好算法是并行的 Pollard ρ 算法，表 3.2 给出了 RSA 和 ECC 安全强度的比较 (MIPS 年是指一台每秒执行 1000 000 条指令的计算机一年的计算量)：

表 3.2 RSA 和 ECC 安全强度的比较

RSA 模数	ECC 基域	MIPS 年
1024bit	163bit	10^{12}
2048bit	211bit	10^{20}

目前,利用网络资源,国际上已经解决了 Certicom 所给出的基域尺寸为 109bit 的 ECDLP 挑战，这也是已有的最好结果，其所用资源如表 3.3 所列 (2K-108 表示特征为 2 、基域尺寸为 108bit 且是 Koblitz 曲线， 2-109 表示特征为 2 、基域尺寸为 109bit ， p-109 表示基域的阶为 109bit 的素数).

表 3.3 所用资源表

基域	算法	解决的日期	计算机的个数	花费的时间
2K-108	并行 Pollard rho	2000 年 4 月	9 500	4 月
p-109	并行 Pollard rho	2002 年 11 月	10 000	549 天
2-109	并行 Pollard rho	2004 年 4 月	2 600	17 月

3.6.2 Diffie-Hellman 密钥交换协议

密钥交换协议使得在不安全信道的多个用户获得共同的秘密信息，该信息将可能作为对称密码体制的私钥，而攻击者无法得到该密码信息. Diffie-Hellman 密钥交换协议的细节如下.

(1) 用户 A 和 B 选择并公开一组系统参数 $(q, \mathbb{F}_q, E, P, n)$： $q \in \{p, 2^m\}$ ，p 为大素数，有限域 $\mathbb{F}_q$ ，其上的安全椭圆曲线群 E ，以及某个阶为大素数 n 的点 $P \in E(\mathbb{F}_q)$.

(2) 用户 A(B) 选择随机数 $a(b) \in \mathbb{Z}_n$ ，计算 $Q_a = aP(Q_b = bP)$ ，并将其发送给对方.

(3) 用户 A 和 B 利用各自的随机数和从对方获取的信息，可以计算得到 $S = abP$, 即

$$S = a(Q_b) = b(Q_a),$$

则 S 便是用户 A 和 B 共有的密钥.

如果攻击者可以窃听，则他知道 P, Q_a, Q_b ，为了获得密钥 S ，攻击者必须由 $P, Q_a = aP, Q_b = bP$ 求得 $S = abP$ ，这是椭圆曲线计算 Diffie-Hellman 问题 (ECCDHP). 如果椭圆曲线离散对数问题可解，即对于输入 Q ，存在多项式时间的算法求得 k, 使得 $Q = kP$ ，则 ECCDHP 可解. 其逆命题，即 ECCDHP 可解，则 ECDLP 可解，是否成立目前仍是一个公开的问题.

3.6.3 ElGamal 加密体制

设 E 为有限域 $\mathbb{F}_q$ 上的安全椭圆曲线群， $P \in E(\mathbb{F}_q)$ ， P 的阶为大素数 n ， $q \in \{p, 2^m\}$ ，用户 A 的私钥为 $d_a \in \mathbb{Z}_n$ ，公钥为 $Q_a = d_a P$. 若用户 B 想发送明文 m 给用户 A：

(1) B 随机选择 $k \in \mathbb{Z}_n$ ；

(2) B 计算 $C_1 = kP, R = kQ_a$ ， R 的 X 坐标记为 $x(R)$ ；

(3) B 计算 $c_2 = mx(R)$.

(4) B 发送密文 $C = (C_1, c_2)$ 给 A.

用户 A 收到密文 C 后,利用自己的私钥 d_a ,计算 $R = d_a C_1, m = c_2 x(R)^{-1}$ ，便获得了明文 m.

显然，若 ECCDHP 可解，则攻击者可以由 C_1, Q_a 求得 R ，进而获得明文 m ，所以 ElGamal 加密体制是基于 ECCDHP 的. ElGamal 加密体制并不安

全：设 $m' = m\delta$，则 $C' = (C_1, c_2\delta)$ 是 m' 的密文，即攻击者获得了明文 m 的密文 C 后，他可以伪造任意明文的密文.

3.6.4 ECDSA

1994 年，美国国家标准和技术局 (National Institute for Standards and Technology of the USA, NIST) 公布了数字签名标准 (Standard for Digital Signature, DSS)，其核心为数字签名算法 (Algorithm for Digital Signatures, DSA). 以下给出椭圆曲线数字签名算法 ECDSA：

设 E 为有限域 $\mathbb{F}_q$ 上的安全椭圆曲线群，$P \in E(\mathbb{F}_q)$，P 的阶为大素数 n，$q \in \{p, 2^m\}$，用户 A 的私钥为 $d_a \in \mathbb{Z}_n$，公钥为 $Q_a = d_aP$，$H(.)$ 为 hash 函数. 用户 A 执行如下操作对消息 m 签名：

(1) 随机选取 $k \in \mathbb{Z}_n$;

(2) 计算 $R = kP$，R 的 X 坐标记为 $x(R)$，$c = x(R) \mod n$；

(3) $s = k^{-1}(H(m) + d_a c) \mod n$；

(4) 消息 m 的签名为 (m, c, s).

用户 B 得到签名 (m, c, s) 后，执行如下操作验证其合法性：

(1) 计算 $k_1 = H(m)s^{-1} \mod n, k_2 = cs^{-1} \mod n$；

(2) 计算 $R' = k_1P + k_2Q_a$；

(3) 若 $c = x(R') \mod n$，则通过验证；否则，认为该签名非法.

如果 ECDLP 可解，则攻击者能够获得用户 A 的私钥 d_a，显然他可以对任意消息伪造 A 的签名，故 ECDSA 是基于 ECDLP 的. ECDSA 可以划归为 ElGamal 类签名体制，而 ElGamal 类签名体制共有 1000 余种签名算法，读者可以参阅文献 [50].

习 题 三

3.1 令 $f, g \in K(E)$ 使得 $\text{div}(f)$ 和 $\text{div}(g)$ 无相同的支撑点，则

$$f(\text{div}(g)) = g(\text{div}(f)).$$

3.2 对于 m 扭点 S, T，有 $e_m(S,T) = \dfrac{f_S(D_T)}{f_T(D_S)}$.

3.3 设 D 是零次除子，且 $kP, 0 \leqslant k < n$ 均不属于 D 的支撑，令 $U = \{kP : 0 \leqslant k < n\} \times \bar{\mathbb{F}}_q^{\times}$，其上的加法 $\oplus$ 为

$$(k_1P, c_1) \oplus (k_2P, c_2) = ((k_1 + k_2)P, c_1c_2h(D)),$$

$$h = \frac{l_{k_1P,k_2P}}{v_{(k_1+k_2)P}},$$

其中，l_{k_1P,k_2P} 为 k_1P, k_2P 所决定的直线，$v_{(k_1+k_2)P}$ 为过 $(k_1+k_2)P$ 的垂线，则 $(U,\oplus)$ 为群.

3.4 设 D 是零次除子，且 $kP, 0 \leqslant k < n$ 均不属于 D 的支撑，$k\odot(P,1)$ 表示 k 个 $(P,1)$ 进行 $\oplus$ 运算，则 $k\odot(P,1) = (kP, g_k(D))$，其中

$$\mathrm{div}(g_k) = k < P > - < kP > -(k-1) < O > .$$

3.5 设 E 是超奇异椭圆曲线，$E(\mathbb{F}_q) \simeq \mathbb{Z}_{n_1} \times \mathbb{Z}_{n_2}, n_1|n_2$，则 $E(\mathbb{F}_{q^k}) \simeq \mathbb{Z}_{cn_2} \times \mathbb{Z}_{cn_2}$，其中 R 为满足 $E[n_2] \subseteq E(\mathbb{F}_{q^k})$ 的最小整数.

表 3.4 习题 3.5 表

$t = q+1-\lvert E(\mathbb{F}_q)\rvert$	群结构	n_2	k	c
0	循环	$q+1$	2	1
0	$\mathbb{Z}_2 \times \mathbb{Z}_{\frac{q+1}{2}}$	$\frac{q+1}{2}$	2	2
$\pm\sqrt{q}$	循环	$q+1\mp\sqrt{q}$	3	$\sqrt{q}\pm 1$
$\pm\sqrt{2q}$	循环	$q+1\mp\sqrt{2q}$	4	$q\pm\sqrt{2q}+1$
$\pm\sqrt{3q}$	循环	$q+1\mp\sqrt{3q}$	6	$\frac{q+1}{q+1\pm\sqrt{3q}}$
$\pm 2\sqrt{q}$	$\mathbb{Z}_{\sqrt{q}\mp 1} \times \mathbb{Z}_{\sqrt{q}\mp 1}$	$\sqrt{q}\mp 1$	1	1

第 4 章　椭圆曲线求阶算法

椭圆曲线密码体制中系统参数的选取要求能够得到椭圆曲线上的一个点 P，且其阶是大素数. 通用的方法有两种：一种是先确定椭圆曲线的阶，再寻找椭圆曲线，最后确定阶为大素数的点；另一种是先随机选取椭圆曲线，再确定其阶，若阶没有大的素数因子，则舍弃该曲线，并重新选择椭圆曲线；否则，确定阶为大素数的点. 由于后一种算法具有较好的随机性，故得到了广泛的应用. 而其中最核心的问题便是求取椭圆曲线的阶. 以下均假设 $k = \mathbb{F}_q = \mathbb{F}_{p^m}$， E 是定义在 k 上的椭圆曲线.

目前，有限域上有效的求阶算法可归为 3 类.

(1) SEA 算法　1985 年, Schoof[116] 首先提出了一个时间复杂度为 $O(\log^8 q)$ 的多项式时间的求阶算法，随后， Elkies 和 Atkin 改进了该算法 [5,6,30]，大大提高了实现效率，其时间复杂度为 $O(\log^6 q)$，现人们常称之为 SEA(Schoof-Elkies-Atkin) 算法. 对于特征为 2 的有限域 $\mathbb{F}_{2^n}$ 上的椭圆曲线， Couveignes[23,24] 和 Lercier[71] 利用了 $\mathbb{F}_{2^n}$ 上椭圆曲线的特性，更细致地刻划了 SEA 的相关结果，局部优化了 SEA 算法，使其实现效率得到进一步提高 [21,53,73].

(2) Satoh 算法　2000 年， Satoh[109] 对于特征大于等于 5 的有限域上的椭圆曲线的求阶提出了一种新的算法： Satoh 算法. 随后， Skjernaa[130] 及 Fouquet,Gaudry 和 Harley[34] 分别独立地将该算法推广到特征为 2 的有限域上的椭圆曲线阶的计算，其时间复杂度为 $O(\log^5 q)$，空间复杂度为 $O(\log^3 q)$. 2001 年，Vercautern 等人 [140] 巧妙地利用牛顿插值公式及 j 不变量间的关系，把 Satoh 算法的存储空间减小为 $O(\log^2 q)$，运算时间提高了 1.5 倍. 同年，Satoh,Skjernaa, Taguchi[112] 利用文献 [140] 中的结论，将提升 j 不变量的计算复杂度由 $O(\log^5 q)$ 减小为 $O(\log^{13/3} q)$，他们结合 Satoh 算法的思想和求取范数的算法，提出了 SST 算法，其时间复杂度为 $O(\log^{4.5} q)$，空间复杂度为 $O(\log^2 q)$.

(3) AGM 算法　2001 年， Harley,Mestre 和 Gaudry[48] 基于算术几何平均方法 (arithmetic geometric mean)，给出了一个完全不同的求阶算法： AGM 算法，其空间复杂度为 $O(\log^2 q)$，运行时间比 Vercautern 等人的算法 [140] 提高了一个常数. 2002 年，Gaudry[40] 综合 AGM 算法和 SST 算法，提出了 MSST

算法 (the modified SST algorithm)，其空间复杂度为 $O(\log^2 q)$，运行时间比 AGM 算法提高了一个常数.

由于 Satoh 算法、SST 算法和 AGM 算法都是采用把 $\mathbb{F}_q$ 上椭圆曲线提升到 p-daic 域 $\mathbb{Q}_q$ 上再求取阶的思路，人们常将它们统称为 p-adic 求阶方法. 而 SEA 算法采用先求 $\mathbb{F}_q$ 上椭圆曲线群的阶模小素数 l 的局部信息，再综合成整体结论的思路，被称为 l-adic 求阶方法. 因为 p-adic 求阶方法的计算复杂度前的常数和域的特征 p 有密切的关系，所以当 p 较大时， SEA 算法比 p-adic 求阶方法有效，即计算特征为大素数的域上椭圆曲线群的阶目前适用的算法仍是 SEA 算法. 而当 $p=2$ 时，最高效的求阶算法为 p-adic 方法中的 MSST 算法. 本章首先介绍 SEA 算法，然后对于特征为 2 的有限域，介绍 Satoh 算法和 AGM 算法.

4.1 Schoof 算法

第一个多项式时间的椭圆曲线求阶算法是 Schoof 于 1985 年提出的，它是一个确定性算法 [116]，其理论基石便是 Hasse 定理.

令 $t=q+1-|E(k)|, \varphi:(x,y)\mapsto(x^q,y^q)$ 是 Frobenius 自同态，则 t 是满足式 (4.1) 的唯一的整数

$$\varphi^2-t\varphi+q=0; \tag{4.1}$$

而且由定理 2.8.1 知

$$|t|\leqslant 2\sqrt{q}.$$

所以，只需要对于大于 $4\sqrt{q}$ 的任意整数 L 确定 $t \mod L$，即可得 t 的取值. 那么问题可以转化为几个子问题：寻找一个由素数 $l\neq 2,p$ 组成的集合，且集合中所有素数的乘积大于 $4\sqrt{q}$；对于集合中的每一个素数 l 确定 $t \mod l$，然后利用中国剩余定理即可求得 t.

确定 $t \mod l$ 时，将式 (4.1) 限制在 $E[l]$ 上得

$$\varphi_l^2-\tau\varphi_l+s=0, \tag{4.2}$$

其中 φ_l 是 φ 限制在 $E[l]$ 上， $s\equiv q \mod l, \tau\equiv t \mod l$. 对于 $0\leqslant\tau<l$，判断该式是否成立，若 τ_0 满足，则 $t\equiv\tau_0 \mod l$. 判断过程利用了可除多项式 ψ_l.

引理 4.1.1 设奇素数 $l\neq p, f=u+vY\in k[E], u,v\in k[X]$，则下列条件等价：

(1) 对于任意的 $P \in E[l]$，有 $f(P) = 0$;

(2) 在 $k[X]$ 中，ψ_l 整除 u, v.

证明 由推论 2.6.5 知 $\psi_l \in k[X]$，所以该引理是有意义的. 由命题 2.6.8 知

$$\text{div}\psi_l = < E[l] > -l^2 < O >$$

所以 f 作用于 $E[l]$ 恒为 0，当且仅当 $\dfrac{f}{\psi_l}$ 没有有限极点，即 $\dfrac{f}{\psi_l} \in k[E]$. 设 $\dfrac{f}{\psi_l} = a + bY, a, b \in k[X]$，则 $f = u + vY = a\psi_l + b\psi_l Y$，故 $u = a\psi_l, v = b\psi_l$.

由该引理知，判断多项式函数作用于 $E[l]$ 是否恒为 0 转化为判断该式 (正规型) 是否能被 ψ_l 整除. 如果多项式函数比较特殊，则容易验证 l 阶点是否是其零点.

引理 4.1.2 设奇素数 $l \neq p, f \in k[E]$，$f \in k[X]$ 或 $\dfrac{f}{\psi_2} \in k[X]$. 令

$$\tilde{f} = \begin{cases} f, & f \in k[X] \\ \dfrac{f}{\psi_2}, & \text{其他} \end{cases}$$

则下述条件等价:

(1) 存在点 $P \in E[l]$ 使得 $f(P) = 0$.

(2) $\gcd(\tilde{f}, \psi_l) \neq 1$.

证明 设 $f \in k[X], P = (x, y) \in E[l], f(P) = 0$. 则在 $k[X]$ 中有 $X - x$ 整除 f. 另一方面 $\psi_l(P) = 0$，所以在 $k[X]$ 中 $X - x$ 也整除 ψ_l，故 $\gcd(f, \psi_l) \neq 1$. 若 $\gcd(f, \psi_l) \neq 1$，不妨设 $X - x$ 整除 $\gcd(f, \psi_l)$，则存在点 $P = (x, y) \in E[l]$，使得 $\psi_l(P) = 0, f(P) = 0$. 设 $f = \psi_2\tilde{f}, \tilde{f} \in k[X]$，因为 l 是奇素数，所以对于任意 $P \in E[l]$，$\psi_2(P) \neq 0$，因此对于 l 阶点 P，$f(P) = 0$ 等价于 $\tilde{f}(P) = 0$. 再由上一种情况的结论，即得所证结论.

判断式 (4.2) 是否成立时，需要将 φ_l^2, s 相加，故首先需要判断 φ_l^2 是否等于 $\pm s$.Schoof 的原始算法，是利用引理 4.1.2 来判断是否存在 l 阶点 P, 使得 $\varphi_l^2(P) = \pm sP$，如果结论为否，则 $\varphi_l^2 \neq \pm s$. 但是引理 4.1.2 仅对于特殊的多项式函数有效，而且还需要依据特征的奇偶性来区分算法，故本文采用另一种方法，即利用引理 4.1.1 判断是否对于所有的 l 阶点 P 均有 $\varphi_l^2(P) = \pm sP$. 注意引理 4.1.1 对于 $k[E]$ 中的任意多项式函数均成立，且与特征的奇偶性无关.

第一步：判断 φ_l^2 是否等于 $\pm s$.

$\varphi_l^2 = \pm s$ 的必要条件是在 $E[l]$ 上有 $X(\varphi^2) = X(s)$ ，即在 $E[l]$ 上有 $X^{q^2} - g_s = 0$. 由命题 2.6.3 和命题 2.6.2 知

$$g_s = X - \frac{\psi_{s-1}\psi_{s+1}}{\psi_s^2} \in k(X),$$

利用引理 4.1.1 ，问题转化为判断

$$\psi_s^2(X^{q^2} - X) + \psi_{s-1}\psi_{s+1} \equiv 0 \mod \psi_l$$

是否成立. 若上式不成立，则 $\varphi_l^2 \notin \{s, -s\}$. 否则，分情况讨论.

(1) 如果存在有限点 $P \in E[l]$, 使得 $\varphi_l^2(P) = -sP$ ，则将其代入式 (4.2) 得 $O = \tau_0\varphi_l(P)$ ，因为 $\varphi_l(P) \neq O$ ，且 $\varphi_l(P)$ 为 l 阶点，所以 $\tau_0 = 0$.

(2) 否则， $\varphi_l^2 = s, \tau_0 \neq 0$ ，则由式 (4.2) 知

$$2s = \tau_0\varphi_l \Leftrightarrow \varphi_l = \frac{2s}{\tau_0}, \tag{4.3}$$

其中， τ_0 的逆是在 $\mathbb{Z}_l$ 中求取的. 将 φ_l 代入式 (4.2) 得

$$\frac{4s^2}{\tau_0^2} + s = 2s \Leftrightarrow \tau_0^2 = 4s.$$

因此 τ_0 为 $4s$ 在 $\mathbb{Z}_l = \mathbb{Z}/l\mathbb{Z}$ 中的平方根. 故在该情况下，首先判断 s 是否是 $\mathbb{Z}_l$ 中的二次剩余，即 $\left(\frac{s}{l}\right)$ 是否等于 1 ，如果不等于 1 ，则 $\varphi_l^2 = -s, \tau_0 = 0$ ；否则，设 ω 是 s 的平方根 (可以通过穷举求得) ，由式 (4.3) 知接下来需要判断 φ_l 是否等于 $\pm\omega$. 若

$$\psi_\omega^2(X^q - X) + \psi_{\omega-1}\psi_{\omega+1} \equiv 0 \mod \psi_l \tag{4.4}$$

不成立，则 $\varphi_l^2 = -s, \tau_0 = 0$. 否则， $\varphi_l^2 = s$ ，需要判断 φ 等于 ω 还是 $-\omega$. 由命题 2.6.6 知

$$h_\omega = Y + \frac{\psi_{\omega+2}\psi_{\omega-1}^2}{\psi_2\psi_\omega^3} + (3X^2 + 2a_2X + a_4 - a_1Y)\frac{\psi_{\omega-1}\psi_{\omega+1}}{\psi_2\psi_\omega^2},$$

通分得

$$\psi_2\psi_\omega^3(Y(\varphi_l) - Y(\omega)) \tag{4.5}$$

$$= \psi_2\psi_\omega^3(Y^q - h_\omega) \tag{4.6}$$

$$= \psi_2\psi_\omega^3(Y^q - Y) - \psi_{\omega+2}\psi_{\omega-1}^2 - (3X^2 + 2a_2X + a_4 - a_1Y)\psi_{\omega-1}\psi_\omega\psi_{\omega+1}, \tag{4.7}$$

通过化简可得多项式 $u+vY, u,v \in k[X]$. 如果 ψ_l 整除 u,v ,则 $\varphi_l=\omega, \tau_0=2\omega$;否则, $\varphi_l=-\omega, \tau_0=-2\omega$.

第二步：如果第一步测试失败，即 $\varphi_l^2 \neq \pm s$ ，则 $\varphi^2 \neq \pm s$ ，所以可以利用加法公式得 φ^2+s ：

$$\begin{aligned}
\alpha &= \psi_2\psi_s^3(Y(\varphi^2)-Y(s)) \\
&= \psi_2\psi_s^3(Y^{q^2}-h_s) \\
&= \psi_2\psi_s^3(Y^{q^2}-Y)-\psi_{s+2}\psi_{s-1}^2 \\
&\quad -(3X^2+2a_2X+a_4-a_1Y)\psi_{s-1}\psi_s\psi_{s+1}, \\
\beta &= \psi_2\psi_s^3(X(\varphi^2)-X(s)) \\
&= \psi_2\psi_s^3(X^{q^2}-g_s) \\
&= \psi_2\psi_s^3(X^{q^2}-X)+\psi_2\psi_{s-1}\psi_{s+1}, \\
\lambda &= \frac{\alpha}{\beta}, \\
g_\varphi &= \psi_s^2\beta^2X(\varphi^2+s) \\
&= \psi_s^2\beta^2(-X^{q^2}-g_s+\lambda^2+a_1\lambda-a_2) \\
&= \psi_s^2(((-X^{q^2}-X-a_2)\beta+a_1\alpha)\beta+\alpha^2)+\beta^2\psi_{s-1}\psi_{s+1}, \\
h_\varphi &= \psi_s^2\beta^3Y(\varphi^2+s) \\
&= -\alpha(g_\varphi-X^{q^2}\psi_s^2\beta^2)-(Y^{q^2}+a_3)\psi_s^2\beta^3-a_1\beta g_\varphi \\
&= \psi_s^2(-(Y^{q^2}+a_3)\beta+\alpha X^{q^2})\beta^2-(\alpha+a_1\beta)g_\varphi.
\end{aligned}$$

在模 ψ_l 下计算出 g_φ, h_φ 后将其储存. 然后，穷尽 $-\frac{l-1}{2} \leqslant \tau \leqslant \frac{l-1}{2}$ ，测试 φ_l^2+s 是否等于 $\tau\varphi_l$ ，直至找到使其相等的 τ ，记为 τ_0. 对于每个正数 τ ，有

$$\begin{aligned}
&\psi_s^2\beta^2\psi_\tau^2(X^q,Y^q)(X(\varphi^2+s)-X(\tau\varphi)) \\
=\ &\psi_\tau^2(X^q,Y^q)g_\varphi-\psi_s^2\beta^2(\psi_\tau^2(X^q,Y^q)X^q-\psi_{\tau-1}(X^q,Y^q)\psi_{\tau+1}(X^q,Y^q)).
\end{aligned}$$

测试该式是否能被 ψ_l 整除. 由于 l 是奇素数，所以 $E[s]\cap E[l]=\{O\}$ ，故 $\gcd(\psi_s^2,\psi_l)=1$ ；同理可得 $\gcd(\psi_\tau^2(X^q,Y^q),\psi_l)=\gcd(\psi_\tau^{2q},\psi_l)=1$ ；若存在 l 阶点 Q, 使得 $\beta(Q)=0$, 因为 $\psi_2(Q)\neq 0, \psi_s^3(Q)\neq 0$, 所以 $\varphi^2(Q)=\pm sQ$, 但是在第二步, 至少存在一个 l 阶点 P 使得 $\varphi^2(P)\neq \pm sP$, 所以若测试通过, 则一定有 $(\varphi^2+s)(P)=\pm\tau\varphi(P)$. 又因为 P 满足式 (4.2) , 即 $(\varphi^2+s)(P)=\tau_0\varphi(P), \varphi(P)$

的阶为 l，所以 $\tau_0 \equiv \pm\tau(\mod l)$. 为了获得 τ_0，还需要比较 Y 坐标：

$$\begin{aligned}
&\psi_s^2\beta^2\psi_2(X^q,Y^q)\psi_\tau^3(X^q,Y^q)(Y(\varphi^2+s)-Y(\tau\varphi))\\
=&\psi_2(X^q,Y^q)\psi_\tau^3(X^q,Y^q)h_\varphi\\
&-\psi_s^2\beta^3(\psi_2(X^q,Y^q)\psi_\tau^3(X^q,Y^q)Y^q+\psi_{\tau+2}(X^q,Y^q)\psi_{\tau-1}^2(X^q,Y^q))\\
&-\psi_s^2\beta^3(3X^{2q}+2a_2X^q+a_4-a_1Y^q)\psi_{\tau-1}(X^q,Y^q)\psi_\tau(X^q,Y^q)\psi_{\tau+1}(X^q,Y^q).
\end{aligned}$$

测试该式是否能被 ψ_l 整除，若测试通过，则 $\tau_0=\tau$；否则 $\tau_0=-\tau$.

注意：在这两个步骤中，对于特征为奇数的情况，可以选取椭圆曲线为正规型，从而简化计算.

算法 4.1(Schoof) 下述算法可以求取 $E(k)$ 的阶，其运行时间为 $O(\log^6 q)$ 次 k 上的乘法和求逆，存储空间为 $O(\log^3 q)$ 个域元素.

(1) 确定素数集合 L，其中的素数不为 $2,p$，且

$$\prod_{l\in L} l > 4\sqrt{q},$$

对于所有的 i,$2\leqslant i\leqslant \max L$，利用命题 2.6.4 递归求得可除多项式 ψ_i. 对于所有的 $l\in L$，利用 (2)~(5) 求取 $\tau_0 \mod l$.

(2) 令 $s=q \mod l$，计算 $X^q \mod \psi_l, X^{q^2} \mod \psi_l, Y^q \mod (E,\psi_l), Y^{q^2} \mod (E,\psi_l)$.

(3) 计算 $\psi_s^2(X^{q^2}-X)+\psi_{s-1}\psi_{s+1} \mod \psi_l$，若不等于 0，转至 (4)；否则，计算 $\left(\frac{s}{l}\right)$. 如果 $\left(\frac{s}{l}\right)=-1$，则 $\tau_0=0$；否则，穷举获得 $\omega\in\mathbb{Z}_l,\omega^2=s$，计算 $\psi_\omega^2(X^q-X)+\psi_{\omega-1}\psi_{\omega+1} \mod \psi_l$，若不等于 0，则 $\tau_0=0$；否则，计算

$$\psi_2\psi_\omega^3(Y^q-Y)-\psi_{\omega+2}\psi_{\omega-1}^2-(3X^2+2a_2X+a_4-a_1Y)\psi_{\omega-1}\psi_\omega\psi_{\omega+1} \mod (E,\psi_l),$$

若等于 0，则 $\tau_0=2\omega$；否则 $\tau_0=-2\omega$. 如果 τ_0 已确定，则返回 (2)，从 L 中选取下一个素数，执行 (2).

(4) 对于 $2\leqslant i\leqslant \frac{l-1}{2}$，利用命题 2.6.4 递归计算 $\psi_i(X^q,Y^q)$.

(5) 在模 ψ_l 下，或模 (E,ψ_l) 下计算：

$$\begin{aligned}
\alpha=&\psi_2\psi_s^3(Y^{q^2}-Y)-\psi_{s+2}\psi_{s-1}^2\\
&-(3X^2+2a_2X+a_4-a_1Y)\psi_{s-1}\psi_s\psi_{s+1},
\end{aligned}$$

$$\beta = \psi_2\psi_s^3(X^{q^2} - X) + \psi_2\psi_{s-1}\psi_s\psi_{s+1},$$
$$g_\varphi = \psi_s^2(((-X^{q^2} - X - a_2)\beta + a_1\alpha)\beta + \alpha^2) + \beta^2\psi_{s-1}\psi_{s+1},$$
$$h_\varphi = \psi_s^2(-(Y^{q^2} + a_3)\beta + \alpha X^{q^2})\beta^2 - (\alpha + a_1\beta)g_\varphi.$$

对于 $1 \leqslant \tau \leqslant \dfrac{l-1}{2}$ ，重复执行如下操作，直至找到 τ_0: 计算

$$\psi_\tau^2(X^q, Y^q)g_\varphi - \psi_s^2\beta^2(\psi_\tau^2(X^q, Y^q)X^q - \psi_{\tau-1}(X^q, Y^q)\psi_{\tau+1}(X^q, Y^q)) \mod (E, \psi_l).$$

若不等于 0 ，则选取下一个 τ ；否则，计算

$$\begin{aligned}
&\psi_s^2\beta^2\psi_2(X^q, Y^q)\psi_\tau^3(X^q, Y^q)(Y(\varphi^2 + s) - Y(\tau\varphi)) \\
=&\ \psi_2(X^q, Y^q)\psi_\tau^3(X^q, Y^q)h_\varphi \\
&-\psi_s^2\beta^3(\psi_2(X^q, Y^q)\psi_\tau^3(X^q, Y^q)Y^q + \psi_{\tau+2}(X^q, Y^q)\psi_{\tau-1}^2(X^q, Y^q)) \\
&-\psi_s^2\beta^3(3X^{2q} + 2a_2X^q + a_4 - a_1Y^q)\psi_{\tau-1}(X^q, Y^q)\psi_\tau(X^q, Y^q)\psi_{\tau+1}(X^q, Y^q) \\
&\quad \mod (E, \psi_l),
\end{aligned}$$

若等于 0 ，则 $\tau_0 = \tau$ ；否则 $\tau_0 = -\tau$.

(6) 利用中国剩余定理求取 $t \in [-2\sqrt{q}, 2\sqrt{q}]$ ，满足对于任意 $l \in L$ 有 $t \equiv \tau_0 \mod l$. 则 $|E(k)| = q + 1 - t$.

以下分析该算法的计算复杂度. 因为 k 上的加法只需要 $O(\log q)$ 次比特运算，乘法和除法均需要 $O(\log^2 q)$ 次比特运算，所以将乘法和除法作为 k 的基本运算.

引理 4.1.3 设 $f, g \in k[X], d_f = \deg\ f \geqslant \deg\ g = d_g, \alpha \in k$ ，则以下操作所需 k 上的基本运算数如下：

(1) $f + g$ 为 0 ；

(2) αf 为 $O(d_f)$;

(3) fg 为 $O(d_f d_g)$;

(4) $f \mod g$ 为 $O((d_f - d_g)d_g)$.

证明 前三个结论显然；设 $f = ag + b, \deg\ b < d_g$ ，则求取 b 的算法相当于计算 ag ，由于 $\deg\ a = d_f - d_g$ ，所以求取 b 需要 $O((d_f - d_g)d_g)$ 次域的基本运算.

引理 4.1.4 设 $f, g, h \in k[E]/(\psi_l), f = f_1 + f_2Y, g = g_1 + g_2Y, h = h_1 + h_2Y, f_1, f_2, g_1, g_2, h_1, h_2 \in k[X]$ 且次数均小于 $\deg \psi_l$ ， $\alpha \in k$ ，则在 $k[E]/(\psi_l)$ 中执行以下操作所需 k 上的基本运算数如下：

(1) $f+g$ 为 0；

(2) αf 为 $O(l^2)$；

(3) fg 为 $O(l^4)$.

证明 已知 ψ_l 的次数为 $\dfrac{l^2-1}{2}\in O(l^2)$. 前两个结论显然；因为

$$\begin{aligned}fg &= (f_1+f_2Y)(g_1+g_2Y)\\ &= f_1g_1+f_2g_2(X^3+a_2X^2+a_4X+a_6)\\ &\quad +(f_1g_2+f_2g_1-f_2g_2(a_1X+a_3))Y,\end{aligned}$$

所以计算 fg 相当于计算固定个数的次数为 $O(l^2)$ 的单变量多项式的乘积，由引理 4.1.3 知需要 $O(l^4)$ 次基本运算，所得乘积多项式模 ψ_l 需要 $O(l^4)$ 次基本运算，所以 fg 需要 $O(l^4)$ 次基本运算.

算法 5.8 的复杂度的证明 Schoof 算法的第一步，假设 $L=\{p_2,\cdots,p_n\}$，其中 p_i 表示第 i 个素数，因为 L 中不能有 $2,p$，所以 L 不包括 $p_1=2$. 由 L 的性质知

$$\prod_{i=2}^{n} p_i > 4\sqrt{q},$$

即

$$\mathcal{V}(p_n) := \log\left(\prod_{i=1}^{n} p_i\right) > \log(8\sqrt{q}).$$

由文献 [107] 的 p70 知

$$\mathcal{V}(p_n) < p_n\left(1+\frac{1}{2\log p_n}\right) < 2p_n.$$

所以只需选取

$$p_n \approx \frac{1}{2}\log(8\sqrt{q}) \in O(\log q),$$

则 ψ_i 列的求取需要 $O(p_n)=O(\log q)$ 次次数至多为 $\dfrac{p_n^2-1}{2}\in O(\log^2 q)$ 的多项式的乘法和除法，因此第一步的计算复杂度为 $O(\log^5 q)$. 对于给定的 l，第二步中 $X^q, X^{q^2}, Y^q, Y^{q^2} \mod \psi_l$ 的计算需要 $O(\log q)$ 次 $k[E]/(\psi_l)$ 中的乘法，故其计算复杂度为 $O(l^4\log q)$. 第三步中需要计算常数次 $k[E]/(\psi_l)$ 中的乘法，相对于此，Legendre 符号 $\left(\dfrac{s}{l}\right)$ 的求取以及模 l 下平方根的求取的计算量可以忽略不计. 而 $k[E]/(\psi_l)$ 中的乘法的运算量为 $O(l^4)$，所以第三步的计算复杂度为 $O(l^4)$.

第四步需要 $O(l)$ 次 $k[E]/(\psi_l)$ 中的乘法，故其计算复杂度为 $O(l^5)$. 第五步中对于给定的 τ，其运算量为 $O(l^4)$，而至多有 $O(l)$ 个 τ，故其计算复杂度为 $O(l^5)$. 因为一共有 $O(\log q)$ 个 l，所以第一步至第五步要重复计算 $O(\log q)$ 次，相对于此，最后中国剩余定理的计算量可以忽略不计，故 Schoof 算法的计算复杂度为 $O(\log^6 q)$ 次基本运算.

在算法执行过程中，需要存储 $O(\log q)$ 个可除多项式和常数个次数不大于 l^2 的多项式，故算法的空间复杂度为 $O(\log^3 q)$.

需要说明的是，$O(\log^6 q)$ 次域上的基本运算相当于 $O(\log^8 q)$ 次比特运算，而 Schoof 的文章中给出的计算复杂度为 $O(\log^9 q)$ 次比特运算，其差异的原因为 Schoof 独立地计算可除多项式

$$\psi_i(X^q, Y^q) = \psi_i(X, Y)^q \mod \psi_l.$$

每一个可除多项式均需要 $O(\log q)$ 次 $k[E]/(\psi_l)$ 中的乘法，即每个的计算量为 $O(\log^5 q)$，一共需要计算 $O(\log q)$ 个，所以总的计算量为 $O(\log^6 q)$ 次域上的基本运算. 而本文给出的算法是递归计算可除多项式的，每一个的计算量为 $O(1)$ 次 $k[E]/(\psi_l)$ 中的乘法，故总的计算量为 $O(\log^5 q)$ 次域上的基本运算.

4.2 Elkies 素数

Atkin 和 Elkies 对 Schoof 算法作了改进，以下三节将介绍其工作，其细节请参看文献 [30],[71],[118].

设 E 是定义在有限域 $k = \mathbb{F}_q$ 上的椭圆曲线，$K = \overline{k}$ 是 k 的代数闭包 奇素数 $l \neq p$，Frobenius 自同态限制在 $E[l]$ 上，满足

$$\varphi_l^2 - \tau_0\varphi_l + s = 0. \tag{4.8}$$

其中 $s \equiv q \mod l$，需要求解 τ_0.Elkies 改进的核心思想是利用可除多项式的因式来求解 τ_0. 因为 ψ_l 在 $\mathbb{Z}[X, a_1, a_3, a_2, a_4, a_6]$ 中不可约，所以 ψ_l 没有对任何椭圆曲线均适用的因式，对于不同的椭圆曲线，必须分别考虑 ψ_l 的分解.

设 $E[l] = S\dot{\cup}\overline{S}\dot{\cup}\{O\}$，其中 $\overline{S} = \{\overline{P} : P \in S\}$，则

$$\psi_l = \prod_{P \in S}(X - X(P)).$$

设存在 $E[l]$ 的非平凡子群 C ，恰好是 E 的 l 阶循环子群，这样的群称为 l 群. 则仿照 ψ_l 可以有如下定义

$$f_C = \prod_{P \in S_C} (X - X(P)) \in K[X],$$

其中 $S_C := S \cap C$ ，则 $C = S_C \dot{\cup} \overline{S_C} \dot{\cup} \{O\}$ ， f_C 是 ψ_l 在 $K[X]$ 中的因式，为了计算方便，希望 $f_C \in k[X]$.

命题 4.2.1 下列条件等价：

(1) $f_C \in k[X]$;

(2) $\varphi_l(C) \subseteq C$;

(3) $\varphi_l(C) = C$, 即 C 在 Frobenius 自同态作用下保持不动；

(4) C 是 φ_l 的特征空间 (eigenspace) ，其特征值 (eigenvalue)$\alpha \in \mathbb{Z}_l^{\times}$.

证明 因为 φ_l 是单映射，所以 (2) 和 (3) 显然等价.

令 $\varphi_{K/k}$ 表示 K/k 的 Frobenius 自同态，以及其在 $K[X]$ 上的典型扩充，即

$$\varphi_{K/k} : \sum_{i=0}^{n} a_i X^i \mapsto \sum_{i=0}^{n} a_i^q X^i,$$

则 $f_C \in k[X]$ 等价于 $\varphi_{K/k}(f_C) = f_C$. 又因为

$$\varphi_{K/k}(f_C) = \prod_{P \in S_C} (X - X(P)^q) = \prod_{P \in S_C} (X - X(\varphi_l(P))),$$

所以等价于 φ_l 将 C 中点的 X 坐标进行了置换，即 C 保持不动，亦即 (1) 和 (3) 等价.

因为 C 是循环群，所以 $\varphi_l(C) = C$ 等价于 C 的生成元 P 被 φ_l 作用到另一个生成元 αP, 由于 φ_l 是单映射，所以 $\alpha \neq 0$ ，即 $\alpha \in \mathbb{Z}_l^{\times}$.

由上知，如果存在 l 群在 Frobenius 自同态作用下保持不动，或等价的，如果 φ_l 有特征值 $\alpha \in \mathbb{Z}_l$ ，则 ψ_l 存在次数为 $\frac{l-1}{2}$ 的因式 $f_C \in k[X]$.

设已经求得 f_C ，则可以通过测试在 C 上 $\varphi_l = \pm\alpha, \alpha \in \left\{1, \cdots, \frac{l-1}{2}\right\}$ 是否成立，来求取特征值. 该测试与 Schoof 算法的第一步类似，仅需要将模 ψ_l 替换为模 f_C. 一旦确定了特征值 α ，则可以求得 τ_0 ：设 P 是特征向量，由式 (4.8) 可知

$$O = (\varphi_l^2 - \tau_0 \varphi_l + s)(P) = (\alpha^2 - \tau_0 \alpha + s)P,$$

因为 P 是 l 阶点，所以在 $\mathbb{Z}_l$ 中有 $\alpha^2-\tau_0\alpha+s=0$ ，则

$$\tau_0=\alpha+s\alpha^{-1}.$$

其中 α^{-1} 是在 $\mathbb{Z}_l$ 中计算的.

在上述过程中还遗留了两个问题：首先，如何确定一个素数 l 是 Elkies 素数？即如何判断 φ_l 在 $\mathbb{Z}_l$ 中有没有特征值？当然，有特征值意味着 φ_l 的特征多项式 $X^2-\tau_0X+s$ 在 $\mathbb{Z}_l$ 中有根，即 τ_0^2-4s 不是 $\mathbb{Z}_l$ 中的非二次剩余，所以大约有一半的素数 $l\in L$ 是 Elkies 素数，但是在不知道 τ_0 的条件下，是无法使用该判别条件的. 其次，在不分解 ψ_l 的条件下，如何求得 f_C ？这些问题将在下节给出解决方法.

4.3 同种映射和模多项式

本节将解决是否存在 Frobenius 自同态作用下保持不动的 l 群的问题. 首先证明了 φ_l 对 l 群的作用可以由椭圆曲线 E/C 的 j 不变量来刻画，其中从 E 到 E/C 存在核为 C 的同种映射 (isogeny). 然后，将原问题转化为判断一个多项式是否在 $k[X]$ 中有根.

椭圆曲线间的同种关系是一个等价关系：反身性和传递性显然；已有结论，如果 $\alpha\in E'(K(E))$ 是 m 次同种，则存在同种映射 $\hat{\alpha}\in E(K(E'))$ ，使得 $\hat{\alpha}\circ\alpha=[m]$ ，所以“同种的”也具有对称性.

因为 (α_1,α_2) 的核由 α_1 或 α_2 的极点组成，而有理函数只有有限个极点，所以任意非零同种映射的核均有限. 反之， Vélu 在文献 [139] 中证明了对于 E 的任意有限子群 C ，存在椭圆曲线 E' 和核为 C 的同种映射 $\alpha\in E'(K(E))$ ，且在同构意义下， E' 是唯一的. α 如下：

$$\alpha_1(P)=X(P)+\sum_{Q\in C\setminus\{O\}}(X(P+Q)-X(Q));$$
$$\alpha_2(P)=Y(P)+\sum_{Q\in C\setminus\{O\}}(Y(P+Q)-Y(Q)).$$

用 3.1 节的表示，则为

$$\alpha_1=\sum_{Q\in C}X\circ\tau_Q-c_1, \text{和 } \alpha_2=\sum_{Q\in C}Y\circ\tau_Q-c_2;$$

$$c_1 = \sum_{Q \in C \backslash \{O\}} X(Q) \in K \text{ 和 } c_2 = \sum_{Q \in C \backslash \{O\}} Y(Q) \in K.$$

因为 C 有限，$X \circ \tau_Q, Y \circ \tau_Q$ 是有理函数，所以 α_1, α_2 是有理函数. 对于任意点 $P \in C$，因为 τ_Q 是非分歧的，所以

$$\begin{aligned}
&\mathrm{ord}_P\left(\sum_{Q \in C \backslash \{-P\}} X \circ \tau_Q - c_1\right) \geqslant 0;\\
&\mathrm{ord}_P(X \circ \tau_{-P}) = e(\tau_{-P})\mathrm{ord}_O(X) = -2;\\
&\mathrm{ord}_P(\alpha_1) = \mathrm{ord}_P\left(X \circ \tau_{-P} + \sum_{Q \in C \backslash \{-P\}} X \circ \tau_Q - c_1\right) = -2;\\
&l(\alpha_1) = \left(\left(\frac{X}{Y}\right)^2 \alpha_1\right)(O) = \frac{X^3}{Y^2}(O) = 1.
\end{aligned}$$

同理可知 $\mathrm{ord}_P(\alpha_2) = -3, l(\alpha_3) = 1$，所以 $\alpha_2^2 - \alpha_1^3$ 在 O 的极点重数至多为 5. 如果极点重数恰为 5，则 $\alpha_2^2 - \alpha_1^3 - l(\alpha_2^2 - \alpha_1^3)\alpha_1\alpha_2$ 在 O 的极点重数至多为 4，同理依次加上 $\alpha_1^2, \alpha_2, \alpha_1, 1$ 的适当的倍数，则得到以 O 为零点的有理函数，即

$$E'(\alpha_1, \alpha_2) = \alpha_2^2 + a_1'\alpha_1\alpha - 2 + a_3'\alpha_2 - (\alpha_1^3 + a_2'\alpha_1^2 + a_4'\alpha_1 + a_6').$$

对于 C 中的任意点 P，$\alpha_1 \circ \tau_{-P} = \alpha_1, \alpha_2 \circ \tau_{-P} = \alpha_2$，所以

$$\mathrm{ord}_P(E'(\alpha_1, \alpha_2)) = \mathrm{ord}_P(E'(\alpha_1, \alpha_2) \circ \tau_{-P}) = \mathrm{ord}_O(E'(\alpha_1, \alpha_2)) \geqslant 0,$$

即 C 中的点均是 $E'(\alpha_1, \alpha_2)$ 的零点，所以 $E'(\alpha_1, \alpha_2)$ 没有极点，故 $E'(\alpha_1, \alpha_2)$ 为常值，进一步，$E'(\alpha_1, \alpha_2)$ 为 0. 可以证明 E' 是非奇异的，因此 E' 定义了一条椭圆曲线. 由 $E' \circ \alpha = 0$，可知 α 是 E 到 E' 的一个有理映射，因为 $\alpha(O) = O$，所以 α 是同种映射 [126](SectionII.4).

利用加法公式先求得 $X \circ \tau_Q, Y \circ \tau_Q$ 的有理函数表达式，进而可以获得 α_1, α_2 的有理函数表达式. 本文仅给出结果，详细计算请读者完成. 令 $C = S \dot\cup \bar{S} \dot\cup R \dot\cup \{O\}, R = (E[2] \cap C) \setminus \{O\}$.

$$\begin{aligned}
DX &= 2Y + a_1X + a_3;\\
DY &= 3X^2 + 2a_2X + a_4 - a_1Y;
\end{aligned}$$

$$t(Q) = \begin{cases} DY(Q), & Q \in R; \\ (2DY + a_1DX)(Q), & Q \in S\dot{\cup}\overline{S}; \end{cases}$$
$$u(Q) = (DX)^2(Q);$$
$$t = \sum_{Q\in S\dot{\cup}R} t(Q);$$
$$u = \sum_{Q\in S\dot{\cup}R} (u(Q) + X(Q)t(Q)).$$

若 $Q \notin E[2]$，则 $t(Q) = t(\overline{Q}), u(Q) = u(\overline{Q})$，故以上表达式与 S 的选择无关.

$$\alpha_1 = X + \sum_{Q\in S\dot{\cup}R} \left(\frac{t(Q)}{X - X(Q)} + \frac{u(Q)}{(X - X(Q))^2}\right), \tag{4.9}$$

$$\begin{aligned}\alpha_2 = Y - \sum_{Q\in S\dot{\cup}R} \Bigg(&u(Q)\frac{DX}{(X - X(Q))^3} + t(Q)\frac{a_1(X - X(Q)) + Y - Y(Q)}{(X - X(Q))^2} \\ &+ \frac{a_1u(Q) + DX(Q)DY(Q)}{(X - X(Q))^2}\Bigg),\end{aligned}$$
$$a_1' = a_1,$$
$$a_3' = a_3,$$
$$a_2' = a_2,$$
$$a_4' = a_4 - 5t,$$
$$a_6' = a_6 - (a_1^2 + 4a_2)t - 7u.$$

实际上 c_1, c_2 是可以任意选择的.

l 群 C 可以确定一条椭圆曲线 E/C，使得从 E 到 E/C 存在核为 C 的同种映射. 令 j/C 表示 E/C 的 j 不变量, 因为 E/C 在同构意义下是唯一的, 所以 j/C 是良定义的 (well-defined).C 在 Frobenius 自同态的幂次作用下保持不动的性质与 j/C 密切相关.

定理 4.3.1　设 E 是定义在 k 上的非超奇异椭圆曲线, 且不与 j 不变量为 $0, 1728$ 的椭圆曲线是 k 同种的, 令 C 为 l 群, 则对于正整数 d 下列条件等价:

(1) $\varphi_l^d(C) = C$;

(2) $j/C \in \mathbb{F}_{q^d}$.

证明 设 φ_l^d 是 C 到 C 的双映射，要证 $j/C \in \mathbb{F}_{q^d}$，只需证 $t, u \in \mathbb{F}_{q^d}$. 注意到 φ_l 不改变点的阶，即 $P \in C$ 和 $\varphi_l(P)$ 的阶相同，则

$$\begin{aligned} t^{q^d} &= \sum_{Q \in S \dot{\cup} R} t(Q)^{q^d} = \sum_{Q \in S \dot{\cup} R} t(\varphi_l^d(Q)) \\ &= \sum_{Q \in \varphi_l^d(S) \dot{\cup} \varphi_l^d(R)} t(Q). \end{aligned}$$

又因为 φ_l^d 是 C 上的双映射，所以 $\varphi_l^d(R) = R, C = \varphi_l^d(S) \dot{\cup} \overline{\varphi_l^d(S)} \dot{\cup} R \dot{\cup} \{O\}$，故 $t^{q^d} = t$. 同理可以证明 $u^{q^d} = u$，所以 $j/C \in \mathbb{F}_{q^d}$.

设 $j/C \in \mathbb{F}_{q^d}$，要证明 $\varphi_l^d(C) = C$，其证明过程利用了椭圆曲线自同态环，超出了本书范围. 请见文献 [97],Satz 3.10.

上述定理说明了在 Frobenius 自同态作用下保持不动的 l 群的存在性等价于

$$\prod_{C\ l\text{群}} (X - j/C)$$

在 k 中有根. 该多项式可以在不知道 j/C 的条件下计算得到.

定义 4.3.2 *存在具有以下性质的多项式 $\Phi_l \in \mathbb{Z}[X, Y]$：如果 E 是定义在 k 上的非超奇异的椭圆曲线，其 j 不变量不等于 $0, 1728$，则*

$$\Phi_l(X, j(E)) = \prod_{C\ l\text{群}} (X - j/C).$$

$\Phi_l(X, j(E))$ 是 $l+1$ 次的，有互不相同的根. 称 Φ_l 为 l-th 模多项式 (l-th modular polynomial).

证明 请参看文献 [97],Satz 4.13 和 Lemma 4.14. 由 Φ_l 是 $l+1$ 次的，所以有 $l+1$ 个不同的 l 群，而 l 阶点的个数为 l^2-1，故每个 l 群有 $l-1$ 个生成元.

推论 4.3.3 *设 E 是定义在 k 上的非超奇异椭圆曲线，且与 j 不变量为 $0, 1728$ 的椭圆曲线不是 k 同种的，则在 φ_l^d 作用下保持不动的 l 群的数量为 $\deg(\gcd(X^{q^d} - X, \Phi_l(X, j(E))))$.*

证明 由定理 4.3.1 知在 φ_l^d 作用下保持不动的 l 群的个数为属于 $\mathbb{F}_{q^d}$ 的 j/C 的个数，即为 $\Phi_l(X, j(E))$ 在 $\mathbb{F}_{q^d}$ 中根的个数. 又因为

$$X^{q^d} - X = \sum_{x \in \mathbb{F}_{q^d}} (X - x),$$

所以结论成立.

至此，上一节所遗留的第一个问题便得以解决了，模多项式的计算是非常耗时的，它需要某一类模形式的 Fourier 序列展开，请参看文献 [97] Chapter 4 和 5. 但是模多项式可以预计算获得，然后存储在硬盘上，以后的算法便只需要调用模多项式.

一旦确定 l 是 Elkies 素数，即存在在 φ_l 作用下保持不动的 l 群 C ，便可由 $\alpha \in E/C(K(E))$ 的精确表达式求得 l-th 可除多项式的因式 f_C. 因为 C 中的点均是 α_1 的 2 重极点，而直线 $X - X(P)$ 的除子为 $<P> + <\overline{P}> - 2<O>$ ，所以在相差一个常数倍的意义下， α_1 的分母为 $\prod_{P \in S}(X - X(P))^2 = f_C^2, C = S\dot{\cup}\overline{S}\dot{\cup}\{O\}$. 计算同种的方法有很多种. 本文仅给出一些参考文献：文献 [71] 的第 4~8 章综述了计算方法；文献 [74] P13 分析了其计算复杂度.

上述问题的解决是基于 Vélu 公式 (4.9) 的，但仍需要在未知 C 下可以解决问题的算法. Elkies 的算法是在复数域上求取同种映射，然后将所得结果通过模 p 约化到有限域上 [97](Chapter 6,7) ，其计算复杂度为 $O(l^2)$. 但是该方法使用了正规型 $Y^2 = X^3 + a_4X + a_6$ ，所以不能适用于 $p \in \{2, 3\}$ 的情况；而且，可能恰好有理数的分母能被小素数整除，所以要求 $p > l$ ，因此该方法适用于特征为大素数的情况. Couveignes 基于椭圆曲线的形式群理论 (formal group) 设计了一个对于任意特征均通用的算法 [26] ，其计算复杂度为 $O(l^3)$. 随后， Lercier 针对 $p = 2$ 的情况设计了具有相同的渐进时间复杂度的算法，其算法简单，实际速度比较快 [70]. 最终， Couveignes 设计了一个通用的时间复杂度为 $O(l^{2+\varepsilon}), \varepsilon > 0$ 的算法 [25].

4.4 Atkin 素数

即使不存在在 φ_l 作用下保持不动的 l 群，仍然有可能获得 τ_0 的部分信息. 命题 4.2.1 指出，当 φ_l 的特征多项式 $X^2 - \tau_0 X + s$ 在 $\mathbb{Z}_l$ 中无根时，该情况会发生，即 $\tau_0^2 - 4s$ 是 $\mathbb{Z}_l$ 的非二次剩余，所以 $X^2 - \tau_0 X + s$ 在 $\mathbb{F}_{l^2}$ 中有两个不同的根 α 和 α^l. 由第 2 章知 φ_l^e 的特征多项式为 $(X - \alpha^e)(X - \alpha^{le})$ ，若其根属于 $\mathbb{Z}_l$ ，则 $\alpha^e = (\alpha^e)^l$ ，即 $(\alpha^{l-1})^e = 1$. 所以使得 l 群保持不动的 φ_l 的最小幂次为 α^{l-1} 在 $\mathbb{F}_{l^2}^\times$ 中的阶 d. 因为 φ_l^d 有两个相同的特征值 $\alpha^d = \alpha^{ld}$ ，而 φ_l 有两个不同的特征值 (形式上) ，所以 φ_l^d 的约当标准型 (Jordan normal form) 是对角

矩阵，所有的 l 群在 φ_l^d 的作用下均保持不动. 再由推论 4.3.3 知， d 是最小的整数，使得 $\Phi_l(X,j(E))$ 整除 $X^{q^d}-X$. 令 $\alpha^{l-1}=\zeta_d$ ， $\mathbb{F}_{l^2}$ 的 d-th 本原单位根，则 ζ_d 有 $\varphi(d)$ 中选择，其中 φ 是 Euler 函数. 因为 $(\alpha^{l-1})^{l+1}=\alpha^{l^2-1}=1$ ，所以 $d|l+1, \varphi(d)\leqslant\varphi(l+1)\leqslant\dfrac{l+1}{2}$. 如果已知 $\mathbb{F}_{l^2}$ 的本原元 $g, \mathbb{F}_{l^2}^{\times}=<g>$ ，则 ζ_d 为 $g^{\frac{l^2-1}{d}i}, \gcd(d,i)=1$. 通常而言，确定本原元并非易事，但对于小素数 l ，可以穷举求得. 而且 ζ_d 也可以事先计算得到并存储在硬盘上. 比较方程系数

$$X^2-\tau_0X+s=(X-\alpha)(X-\alpha^l),$$

得

$$\begin{aligned}\tau_0&=\alpha+\alpha^l=\alpha(1+\zeta_d),\\ \tau_0^2&=\alpha^2(1+\zeta_d)^2,\\ s&=\alpha^{l+1}=\alpha^2\zeta_d.\end{aligned}$$

所以

$$\tau_0^2=\frac{s}{\zeta_d}(1+\zeta_d)^2=s\left(\frac{1}{\zeta_d}+2+\zeta_d\right).$$

由该式知 ζ_d,ζ_d^{-1} 决定了相同的 τ_0^2 ，故 τ_0^2 有 $\dfrac{\varphi(d)}{2}$ 种可能， τ_0 有 $\varphi(d)$ 种可能.

4.5 Schoof-Elkies-Atkin 算法

本节给出了完整的 SEA 算法. 首先需要测试推论 4.3.3 的前提是否成立.

1. 超奇异性测试

由定理 2.12.2 知，特征为 2,3 的情况下，椭圆曲线 E 是超奇异的，当且仅当 $j(E)=0$. 对于其他的特征，定理 2.12.3 罗列了 $|E(k)|$ 的至多五种取值 $n_i, i=1,2,3,4,5$ ，所以可以选取随机点 $P\in E(k)$ ，计算 n_iP ， $i=1,2,3,4,5$ ，若任意的 i ， n_iP 均不为 O ，则 E 是非超奇异的；否则，其可能是超奇异的，不适用于椭圆曲线密码体制.

2. 测试同种于 j 不变量为 $\{0,1728\}$ 的椭圆曲线

设 E 是 k 同种于椭圆曲线 E' ，则由 α 获取 E' 的过程表明了 E' 是定义在 k 上的. 若 E' 的 j 不变量为 $0,1728$ ，则下述定理说明了如何确定 $|E(k)|$.

定理 4.5.1 设 E, E' 是 k 同种的椭圆曲线，且均定义在 k 上，则 $|E(k)| = |E'(k)|$.

证明 设 $\alpha = (\alpha_1, \alpha_2)$ 为 E 到 E' 的 k 同种，φ, φ' 分别是 E, E' 的 Frobenius 自同态. 因为 α_1 的系数属于 k，所以 $\alpha_1(X,Y)^q = \alpha_1(X^q, Y^q)$，同理 $\alpha_2(X,Y)^q = \alpha_2(X^q, Y^q)$，故

$$\varphi' \circ \alpha = (\alpha_1(X,Y)^q, \alpha_2(X,Y)^q) = (\alpha_1(X^q,Y^q), \alpha_2(X^q,Y^q)) = \alpha \circ \varphi.$$

如果 φ 的特征多项式为 $\varphi^2 - t\varphi + q = 0$，则

$$0 = \alpha \circ (\varphi^2 - t\varphi + q) = (\varphi'^2 - t\varphi' + q) \circ \alpha,$$

因为 α 是满射，所以 $\varphi'^2 - t\varphi' + q = 0$，$|E(k)| = |E'(k)|$. 其逆命题也成立，证明请参看文献 [135] Theorem 1(c).

若 $p = 2, 3$，$j(E') = 0$，则 E' 是超奇异的，$|E(k)| = |E'(k)|$，所以 E 也是超奇异的，这在前面已经被排除；若 $p > 3$，可能需要求取 j 不变量为 $0, 1728$ 的曲线的阶，由文献 [97](Chapter9.2) 知该问题相当于在虚二次数域 $\mathbb{Q}(i), \mathbb{Q}(\sqrt{-3})$ 中寻找范数为 q 的元素，然后计算、判断 $E(k)$ 中随机点的相应的倍点是否为 O，若不为 O，则 E 不是 k 同种与 j 不变量为 $0, 1728$ 的曲线；否则，可以利用文献 [97](Chapter11) 求取 $|E(k)|$. 实际上，椭圆曲线密码体制需要使用的是阶为大素数的循环群，如果在上述随机点的测试中，其阶包含大的素因子，则直接可以利用该随机点构造密码体制，而不需要精确求取 $|E(k)|$.

3. 计算 $t \mod l$

若以上两个测试均没有通过，则可以利用上两节的方法对于奇素数 l 计算 $\tau_0 \equiv t \mod l$. 若 l 是 Elkies 素数，可以精确求得 τ_0；若 l 是 Atkin 素数，则可以获得 τ_0 的 $\dfrac{l+1}{2}$ 种可能取值. 因为 f_C 的次数为 $O(l)$，而 ψ_l 的次数为 $O(l^2)$，且由计算同种获得 f_C 的计算复杂度为 $O(l^3)$，所以 Elkies 素数将 Schoof 算法中的计算复杂度 $O(\log^5 q)$ 次域运算降低为 $O(\log^3 q)$ 次.

对于素数幂的算法可以参看文献 [97](Chapter 8) 和文献 [26],[84].

4. 计算 t

设在上述步骤中用到的 Elkies 素数组成的集合为 L_1， Atkin 素数组成的集合为 L_2，令 $l_1 = \prod\limits_{l \in L_1} l, l_2 = \prod\limits_{l \in L_2} l, L = l_1 l_2$，则利用中国剩余定理，可以唯一求

得 $t \mod l_1$ 的值，但 $t \mod l_2$ 有 $\prod_{l \in L_2} v_l$ 种可能取值，其中 v_l 表示 $t \mod l$ 的可能取值个数，所以 t 有 $\prod_{l \in L_2} v_l$ 种可能取值，这一般是 $|L_2|$ 的指数函数.

对于在 $[q+1-2\sqrt{q}, q+1+2\sqrt{q}]$ 中的 t 的可能取值，选取 $E(k)$ 的随机点 P ，计算 tP 是否为 O ，如果仅有一个可能值 t_0 通过测试，则 $q+1-t_0$ 即为 $|E(k)|$ ；否则，需要扩大集合 L_1, L_2. 在实际算法实现中，如果 $L > 4\sqrt{q}$ ，则把第一个通过测试的可能值作为正确值输出.

如果 $|L_2|$ 是关于 $\log q$ 的线性函数，则 Atkin 素数将 Schoof 算法的计算复杂度变为指数级的，但是在目前的使用中，指数时间的 SEA 算法比多项式时间的 Schoof 算法更高效.

4.6 Satoh 算法

近来，Satoh[109] 对于小特征 $p \geqslant 5$ 提出了一个新的运行时间为 $O(\log^{3+\varepsilon} q)$ 的求阶算法，其中有限域 $\mathbb{F}_q$ 中两个元素相乘的计算复杂度为 $O(\log^{\varepsilon} q)$ ，并断言其可以推广到特征为 2 和 3 上， Fouquent, Gaudry 和 Harley 完成了该工作，本文将以上算法通称为 Satoh 算法.

首先介绍 p-adic 整数环 $\mathbb{Z}_p$. 设 π_n 是 $\mathbb{Z}/p^{n+1}\mathbb{Z}$ 到 $\mathbb{Z}/p^n\mathbb{Z}$ 的投射，该投射是环同态，可以将 p-adic 整数定义如下.

定义 4.6.1 一个 p-adic 整数是一个序列 $x = (x_1, x_2, \cdots, x_n, \cdots), x_n \in \mathbb{Z}/p^n\mathbb{Z}$ ，满足 $\pi_n(x_{n+1}) = x_n, n \geqslant 1$.$p$-adic 整数构成的环记为 $\mathbb{Z}_p$.

$\mathbb{Z}_p$ 中的加法和乘法定义为向量的运算. 本节中 $\mathbb{Z}_p$ 均指 p-adic 环. 注意： $\mathbb{Z}_p$ 是离散赋值环，其唯一的非零素理想为 $p\mathbb{Z}_p$ ，其剩余类域 $\mathbb{Z}_p/p\mathbb{Z}_p$ 同构于 $\mathbb{F}_p$.

以下将 π_n 的定义扩展为 $\mathbb{Z}_p$ 到 $\mathbb{Z}/p^n\mathbb{Z}$ 的投射： $x \longmapsto x_n$. 显然，一旦知道 x_n ，则由到 $\mathbb{Z}/p^k\mathbb{Z}$ 的投射容易求得 $x_k, k < n$. 以下令 $\pi = \pi_1$ ， π 可以当作 $\mathbb{Z}_p$ 到 $\mathbb{F}_p$ 的投射.

$\mathbb{Z}_p$ 中的可逆元是不属于 $p\mathbb{Z}_p$ 的元素，即所有的 x 满足 $\pi(x) \neq 0$. 有关 p-adic 整数的详细内容请参见文献 [120](Chapter II).

设 $f(t)$ 是 $\mathbb{Z}_p[t]$ 的 m 次首一多项式，而且 $\pi(f)$ 是 $\mathbb{F}_p[t]$ 的不可约多项式，其中 $\pi(f)$ 是对 $f(t)$ 的系数用 π 作用所得到的多项式.

定义 4.6.2 环 $\mathbb{Z}_q$ 为 $\mathbb{Z}_p[t]$ 模多项式 $f(t)$ 所生成的理想而得到的环.

$\mathbb{Z}_q$ 中的一个元素 a 可以表示为一个多项式 $a_{m-1}t^{m-1} + \cdots + a_1 t + a_0$ ， $\mathbb{Z}_q$

中元素的加法和乘法是模 $f(t)$ 的多项式的加法和乘法. 注意: $\mathbb{Z}_q$ 包含 $\mathbb{Z}_p$ 作为子环 $(a_1 = a_2 = \cdots = a_{m-1} = 0)$.

$\mathbb{Z}_q$ 是非分歧离散赋值环, 其唯一的非零素理想是 $p\mathbb{Z}_q$ 而且剩余类域 $\mathbb{Z}_q/p\mathbb{Z}_q$ 同构于 $\mathbb{F}_q$. 特别地, $\mathbb{Z}_q$ 同构于 Witt 向量组成的环 $W(\mathbb{F}_q)$, Witt 向量的表示方法在理论推导中得到了应用, 但在具体计算时其显得非常不方便.

下面将 π_n 和 π 的定义推广到 $\mathbb{Z}_q$ 上, π 可以理解为到 $\mathbb{F}_q$ 的投射, 以下用"模 p^n" 表述模理想 $p^n\mathbb{Z}_q$. $\mathbb{Z}_q$ 的可逆元是所有的 x 满足 $\pi(x) \neq 0$, 其有关内容可以参见文献 [121](Chapter I 和 II).

定义 4.6.3 *$\mathbb{F}_q$ 上的小 Frobenius 映射是保持子域 $\mathbb{F}_p$ 不动的域同构 $\sigma : x \longmapsto x^p$.*

为了定义提升到 $\mathbb{Z}_q$ 的小 Frobenius 映射 Σ, 还需要介绍一些概念. 需要注意的是虽然 Σ 可以依照下述方法计算, 但其效率非常低. Satoh 算法完全避免了计算 Σ.

首先定义一个考虑了乘法结构的从 $\mathbb{F}_q$ 到 $\mathbb{Z}_q$ 的提升.

定义 4.6.4 *Teichmuller 提升是映射 $\omega : \mathbb{F}_q \to \mathbb{Z}_q$, $\omega(0) = 0$, 对于非零元素 x 定义 $\omega(x)$ 是 $\mathbb{Z}_q$ 中的 $q-1$ 次单位根且满足 $\pi(\omega(x)) = x$.*

该提升的名字来源于 p-adic 分析中的 Teichmuller 特征. Teichmuller 提升可以利用对 $f(X) = X^{q-1} - 1$ 进行 Newton 插值计算得到.

下面再定义 $\mathbb{Z}_q$ 中元素的分解, 这与 Witt 向量的一般表示很相像, 关于 Witt 向量的细节请参见文献 [121] (Chapter 2).

定义 4.6.5 *$x \in \mathbb{Z}_q$ 的准 Witt 分解是唯一满足 $x = \sum_{i \geqslant 0} \omega(x_i)p^i$ 的序列 $(x_i)_{i \geqslant 0}$, $x_i \in \mathbb{F}_q$.*

显然 $x_0 = \pi(x)$, x_i 可以一个一个相继计算获得,即 $x_1 = \pi\left(\dfrac{x - \omega(x_0)}{p}\right), \cdots$.

下面定义 $\mathbb{F}_q$ 的小 Frobenius 映射提升到 $\mathbb{Z}_q$ 得到的 Σ, 显然 $\pi(\Sigma) = \sigma, \sigma$ 是 $\mathbb{F}_q$ 的小 Frobenius 映射, 但是 Σ 不是像 σ 一样的简单的幂运算.

定义 4.6.6 *小 Frobenius 映射 $\Sigma : \mathbb{Z}_q \to \mathbb{Z}_q$ 是如下定义的: 对于任意的 $x \in \mathbb{Z}_q$, 令 $(x_i)_{i \geqslant 0}$ 是其准 Witt 分解, 则 $\Sigma(x)$ 是 $\mathbb{Z}_q$ 中分解为 $(x_i^p)_{i \geqslant 0}$ 的元素, 换而言之, 即为 $\sum_{i \geqslant 0} \omega(x_i^p)p^i$ 或 $\sum_{i \geqslant 0} \omega(x_i)^p p^i$.*

显然, Σ 是环同构. 因为 $\mathbb{Q}_q$ 是 $\mathbb{Z}_q$ 的分式域, 所以 $\Sigma : \mathbb{Z}_q \to \mathbb{Z}_q$ 可以自然地扩展为 $\mathbb{Q}_q$ 到 $\mathbb{Q}_q$ 的域同构, 以下仍用 Σ 表示, 显然 Σ 保持 $\mathbb{Q}_p$ 不动.

对于 $\mathbb{Z}_q$ ，下述的 Newton 插值可以改进多项式的近似解的近似程度. 对于给定的某个精度的解， Newton 插值可以高效地求得一个解，其精度是原精度的两倍. $p^k|x$ 表示 $x \equiv 0 \mod p^k, x \in \mathbb{Z}_q$ ，若 $p^k|x$ 但 $p^{k+1} \nmid x$ ，记 $p^k\|x$ ，则 $p^{-k}x$ 可逆.

令 $x \in \mathbb{Z}_q, f \in \mathbb{Z}_q[t]$ ， k 满足 $p^k\|f'(x)$ ，假设对于某个 $n > k$ ，有 $p^{n+k}|f(x)$ ，则称 x 是 f 精度为 n 的近似解，这意味着存在 f 的解 $y \in \mathbb{Z}_q$ 满足 $x \equiv y \mod p^n$.

首先证明下述引理，说明 Newton 插值将近似解的精度由 n 提高为 $2n-k$.

引理 4.6.7 (Quadratic convergence of Newton iteration) 设 $x \in \mathbb{Z}_q, f \in \mathbb{Z}_q[t]$ ， k 满足 $p^k\|f'(x)$ 且存在某个 $n > k$, 使得 $p^{n+k}|f(x)$. 令

$$\varDelta = \frac{p^{-k}f(x)}{p^{-k}f'(x)}$$

$y = x - \varDelta$ ，则 $y \equiv x \mod p^n, p^{2n}|f(y), p^k\|f'(y)$.

证明 显然 $p^n|\varDelta$ ，所以 $y \equiv x \mod p^n$.Taylor 展开式为

$$f(y) = f(x) - \varDelta f'(x) + \varDelta^2 \varPsi(x),$$

其中, $\varPsi(x)$ 是系数属于 $\mathbb{Z}_q$ 的多项式, 因为 $p^{2n}|\varDelta^2$, 故 $f(y) \equiv f(x) - \varDelta f'(x) \equiv 0 \mod p^{2n}$.

因为 $y \equiv x \mod p^n$ ，所以 $f'(y) \equiv f'(x) \mod p^n$. 又由 $p^k\|f'(x), n > k$ 得 $p^k\|f'(y)$.

推论 4.6.8 设 $z \in \mathbb{Z}_q, f \in \mathbb{Z}_q[t]$, 如果 $2^k\|f'(z)$, 且存在 $n > k$, 使得 $f(z) \equiv 0 \mod 2^{n+k}$ ，则存在 $Z \in \mathbb{Z}_q$ ，使得 $f(Z) = 0$ 且 $Z \equiv z \mod 2^n$.

推论 4.6.9 设 $z \in \mathbb{Z}_q$ 可逆，则以 $z \mod 2$ 的逆为初始值， $k = 0$ ，对 $f(t) = t \cdot z - 1$ 利用 Newton 插值可以求得 z 的任意精度的逆.

推论 4.6.10 设 $x \in \mathbb{Z}_q$ 可逆，如果 x 是模 8 的平方数，则 x 在 $\mathbb{Z}_q$ 中有平方根.

推论 4.6.11 设 $x \in \mathbb{Z}_q$ 可逆，且是 $\mathbb{Z}_q$ 中的平方数， $h \in \mathbb{Z}_q, n \geqslant 4$ ，则选取适当的平方根，有下式成立，即

$$\sqrt{x + 2^n h} \equiv \sqrt{x} + 2^{n-1}\frac{h}{\sqrt{x}} - 2^{2n-3}\frac{h^2}{x\sqrt{x}} \mod 2^{3n-4}.$$

重复应用上述引理，则可以合适的精度的近似解为初值，而得到多项式的所需精度的近似解，这便是 Newton 插值算法.

算法 4.2 (NewtonIterations)

输入 要求的精度 n; 多项式 $f \in \mathbb{Z}_q[t]$; 初始解 $x_0 \in \mathbb{Z}_q$ 和整数 k 满足 $p^k || f'(x_0)$, $p^{2k+1} | f(x_0)$.

输出 $x \in \mathbb{Z}_q$ 满足 $x \equiv x_0 \mod p^{k+1}, p^{n+k} | f(x)$.

(1) If $n \leqslant k+1$ Then $y \leftarrow x_0$; Goto 5;

(2) $n' \leftarrow \left\lceil \dfrac{n+k}{2} \right\rceil$;

(3) $x \leftarrow$ NewtonIterations(n', f, x_0, k);

(4) $y \leftarrow x - \dfrac{p^{-k} f(x)}{p^{-k} f'(x)}$;

(5) Return y.

为了提高实现效率，每一步运算都尽可能用较低的精度，实际上，每一次调用 Newton 插值均减少了精度，要求的精度为 n 的解需调用 Newton 插值 $\log(n)$ 次，如果所有的运算均在精度为 n 下运算，则所需的时间为 $O(M(n)\log(n))$ ，其中 $M(n)$ 表示 $\mathbb{Z}_q$ 中的乘法所需时间；如果最顶层的计算精度为 n ，第一次递归调用的计算精度为 $n/2$ ，第二次调用的计算精度为 $n/4$ 等，则所需的时间为 $O(M(n))$.

而且，当用 Newton 插值计算 $y = x - f(x)/f'(x)$ 时，可以将某些运算的精度减少一半. 以下用 $x + O(p^n)$ 表示任意的 y 满足 $y \equiv x \mod p^n$, 如 $xy + O(p^n)$ 可理解为在精度为 n 下的 xy 值.

若 $a \in \mathbb{Z}_q$ 的精度为 n ，因为 $p^k(a + O(p^n)) = p^k a + O(p^{n+k})$ ，故 $p^k a$ 的精度为 $n+k$. 相反地，若 a 的精度为 n 且有 $p^k | a, k \leqslant n$ ，则 $p^{-k} a$ 的精度为 $n-k$. 当 $p=2$ 时，乘以 p^k 或除以 p^k 可用左移或右移而得到.

因为 $p^k | f'(x)$ ，所以 Newton 插值可利用 $y = x - \Delta + O(p^{2n-k})$ 来计算，其中

$$\Delta = \left(\frac{(f(x) + O(p^{2n})) \cdot p^{-n-k} + O(p^{n-k})}{(f'(x) + O(p^n)) \cdot p^{-k} + O(p^{n-k})} + O(p^{n-k}) \right) \cdot p^n + O(p^{2n-k}).$$

以下开始讨论求阶问题. 设 E 是定义在有限域 k 上的椭圆曲线，已知通过计算 Frobenius 自同态的迹 t 便可以获得 $E(k)$ 的阶 $q+1-t$ ，且 $|t| \leqslant 2\sqrt{q}$.

k 上的小 Frobenius 映射

$$\sigma : k \to k,$$

$$x \mapsto x^p,$$

可扩展为将 E 到共轭曲线 E^σ 的映射:

$$E \to E^\sigma,$$
$$(x,y) \mapsto (\sigma(x), \sigma(y)).$$

其中, E^σ 是对 E 的每个系数用 σ 作用后所得的椭圆曲线, 可以证明该映射是纯不可分的同种映射, 也称为小 Frobenius 映射. 该构造可以继续, 如建立 E^σ 到 E^{σ^2} 的同种等, 重复构造 m 次, 则得到一个同种圈, 最终的椭圆曲线为 E, 记 $E_{m-i} = E^{\sigma^i}, j_{m-i}$ 为 E_{m-i} 的 j 不变量, $i = 1, \cdots, m$; σ_{m-1} 为 E_0 到 E_{m-1} 间的小 Frobenius 映射, σ_i 为 E_{i+1} 到 E_i 的小 Frobenius 映射, 显然 $j_i = j_{i+1}^p$, $i = 0, \cdots, m-2$, 则

$$E_0 \xrightarrow{\sigma_{m-1}} E_{m-1} \xrightarrow{\sigma_{m-2}} \cdots \xrightarrow{\sigma_1} E_1 \xrightarrow{\sigma_0} E_0.$$

定理 4.6.12 E 上的 Frobenius 自同态 $\varphi = \varphi' = \sigma_0 \circ \sigma_1 \circ \cdots \circ \sigma_{m-1}$.

证明 设 $P = (x,y) \in E$, 则 $\varphi'(P) = (\sigma_0 \circ \sigma_1 \circ \cdots \circ \sigma_{m-1})(P) = (\sigma_0 \circ \sigma_1 \circ \cdots \sigma_{m-2})(x^p, y^p) = \cdots = (x^q, y^q) = \varphi(P)$, 所以 $\varphi = \varphi'$.

定义 4.6.13 k 上的椭圆曲线 E 到 $\mathbb{Q}_q$ 的典型提升 (canonical lift)$\mathcal{E}$, 是 $\mathbb{Q}_q$ 上的椭圆曲线, 且满足:

(1) $\mathcal{E}$ 模 2 即为 E;

(2) 在模 2 意义下, $\mathcal{E}$ 的自同态环同构于 E 的自同态环.

定理 4.6.14

(1) E 到 $\mathbb{Q}_q$ 的典型提升 $\mathcal{E}$ 在同构意义下是唯一存在的.

(2) 设 $\mathcal{E}_0, \mathcal{E}_1$ 是 E_0, E_1 到 $\mathbb{Q}_q$ 的典型提升, 则模 2 意义下, $\mathcal{E}_0$ 到 $\mathcal{E}_1$ 的同种环同构于 E_0 到 E_1 的同种环.

(3) 模 2 约化不改变同种的次数.

证明 请见文献 [77].

推论 4.6.15 若 $\mathcal{E}$ 是 E 到 $\mathbb{Q}_q$ 的典型提升, $\mathcal{E}^{\Sigma^i}$ 表示对 $\mathcal{E}$ 的所有系数用 Σ 作用 i 次后所得的曲线, 则 $\mathcal{E}^{\Sigma^i}$ 是 E^{σ^i} 到 $\mathbb{Q}_q$ 的典型提升, 且 $E^{\sigma^{i-1}}$ 到 E^{σ^i} 的小 Frobenius 映射可以提升为 $\mathcal{E}^{\Sigma^{i-1}}$ 到 $\mathcal{E}^{\Sigma^i}$ 的同种, 也称为小 Frobenius 映射, $i \geqslant 0$.

证明 因为对 $\mathcal{E}$ 的自同态的坐标函数中 $\mathbb{Q}_q$ 中的元素用 Σ 作用便得到 $\mathcal{E}^\Sigma$ 的自同态; 而对 $\mathcal{E}^\Sigma$ 的自同态的坐标函数用 Σ^{-1} 作用便得到 $\mathcal{E}$ 的自同态, 且以上

作用互逆，所以 End$\mathcal{E}$ 同构于 End$\mathcal{E}^{\Sigma}$，同理 End$E$ 同构于 End E^{σ}，所以在模 2 意义下， End E^{σ} 同构于 End$\mathcal{E}^{\Sigma}$；而 $\mathcal{E}$ 模 2 即为 E，再利用 Σ 模 2 即为 σ，便知 $\mathcal{E}^{\Sigma}$ 模 2 即为 E^{σ}，所以 $\mathcal{E}^{\Sigma}$ 是 E^{σ} 的典型提升；同理， $\mathcal{E}^{\Sigma^i}$ 是 E^{σ^i} 到 $\mathbb{Q}_q$ 的典型提升．再利用上述定理，可知 $E^{\sigma^{i-1}}$ 到 E^{σ^i} 的小 Frobenius 映射可以提升为 $\mathcal{E}^{\Sigma^{i-1}}$ 到 $\mathcal{E}^{\Sigma^i}$ 的同种，且次数不变．

将 $\mathbb{Z}_q$ 上的小 Frobenius 映射 Σ 可以扩展为 $\mathcal{E}$ 到 $\mathcal{E}^{\Sigma}$ 间的映射，显然该映射即为小 Frobeniu 映射，重复这种作用 m 次，则返回原始曲线 $\mathcal{E}$，获得另一个同种圈， $\mathcal{E}_{m-i}=\mathcal{E}^{\Sigma^i}, J_{m-i}$ 为 $\mathcal{E}_{m-i}$ 的 j 不变量， $i=1,\cdots,m$； Σ_{m-1} 为 $\mathcal{E}_0$ 到 $\mathcal{E}_{m-1}$ 间的小 Frobenius 映射， Σ_i 为 $\mathcal{E}_{i+1}$ 到 $\mathcal{E}_i$ 间的小 Frobenius 映射， $i=0,\cdots,m-2$. 故有（同种曲线圈）：

$$\begin{array}{ccccccccc}
\mathcal{E}_0 & \xrightarrow{\Sigma_{m-1}} & \mathcal{E}_{m-1} & \xrightarrow{\Sigma_{m-2}} & \cdots & \xrightarrow{\Sigma_1} & \mathcal{E}_1 & \xrightarrow{\Sigma_0} & \mathcal{E}_0 \\
\pi\downarrow & & \pi\downarrow & & \cdots\ \pi\downarrow & & \pi\downarrow & & \pi\downarrow \\
E_0 & \xrightarrow{\sigma_{m-1}} & E_{m-1} & \xrightarrow{\sigma_{m-2}} & & \xrightarrow{\sigma_1} & E_1 & \xrightarrow{\sigma_0} & E_0
\end{array}$$

则得到 φ 的提升，即曲线 $\mathcal{E}$ 的自同态 Φ，使得其可交换，形式如下：

$$\begin{array}{ccc}
\mathcal{E} & \xrightarrow{\Phi} & \mathcal{E} \\
\pi\downarrow & & \pi\downarrow \\
E & \xrightarrow{\varphi} & E
\end{array}$$

因为小 Frobenius 映射的对偶同种 $\hat{\sigma}$，以下称为 Verschiebung，是可分的，所以 $\hat{\sigma}$ 完全可以由其核确定，其提升也可由核完全决定．故可通过提升其核，再利用 Vélu 公式 (4.9) 来得到该对偶同种的提升．因此 Satoh 算法利用该对偶同种而不是小 Frobenius 映射．考虑该对偶同种，得到

$$\begin{array}{ccccccccc}
\mathcal{E}_0 & \xrightarrow{\hat{\Sigma}_0} & \mathcal{E}_1 & \xrightarrow{\hat{\Sigma}_1} & & \xrightarrow{\hat{\Sigma}_{m-2}} & \mathcal{E}_{m-1} & \xrightarrow{\hat{\Sigma}_{m-1}} & \mathcal{E}_0 \\
\pi\downarrow & & \pi\downarrow & & \cdots\ \pi\downarrow & & \pi\downarrow & & \pi\downarrow \\
E_0 & \xrightarrow{\hat{\sigma}_0} & E_1 & \xrightarrow{\hat{\sigma}_1} & & \xrightarrow{\hat{\sigma}_{m-2}} & E_{m-1} & \xrightarrow{\hat{\sigma}_{m-1}} & E_0
\end{array}$$

还得到 Frobenius 自同态的对偶同种 $\hat{\varphi}=\hat{\sigma}_{m-1}\circ\hat{\sigma}_{m-2}\circ\cdots\circ\hat{\sigma}_0$ 和其提升 $\hat{\Phi}$：

$$\begin{array}{ccc}
\mathcal{E} & \xrightarrow{\hat{\Phi}} & \mathcal{E} \\
\pi\downarrow & & \pi\downarrow \\
E & \xrightarrow{\hat{\varphi}} & E
\end{array}$$

假设已经求得适当精度下的 E 的提升 $\mathcal{E}$. 因为典型提升保持自同态环不变，所以 Frobenius 映射的迹不变，而且自同态的迹和其对偶的迹相等，则

$$\mathrm{Tr}\varphi=\mathrm{Tr}\Phi=\mathrm{Tr}\hat{\Phi}.$$

由前面的分析知，Φ 可分解为一些小 Frobenius 映射的复合，这些小 Frobenius 映射使得 E 通过 m 次共轭作用后又回到 E，其对偶同种也具有该性质，则

$$\mathrm{Tr}\hat{\Phi}=\mathrm{Tr}(\hat{\Sigma}_{m-1}\circ\hat{\Sigma}_{m-2}\circ\cdots\circ\hat{\Sigma}_0).$$

下一步是分析 Φ 及其对偶所对应的形式群. 以下记 $\mathcal{E}$ 在 O 的一致性参数 $-X/Y$ 为 τ，$\mathcal{E}_i$ 的一致性参数为 τ_i.

定理 4.6.16 设 $\mathcal{E}$ 是定义在 $\mathbb{Z}_q$ 上的椭圆曲线，$\mathcal{F}$ 是 $\mathcal{E}$ 的次数为 d 的同种，$\tau=-\dfrac{X}{Y}$ 是 O 点的一致性参数，假设 $\mathcal{F}$ 模 p 的约化 $\pi(\mathcal{F})$ 是可分的，则 $\mathrm{Tr}(\mathcal{F})=c_1+\dfrac{d}{c_1}$，其中 $\tau\circ\mathcal{F}=\displaystyle\sum_{n=1}^{\infty}c_n\tau^n$.

证明 因为在 $\mathcal{E}$ 的自同态环中有 $\mathcal{F}\circ\mathcal{F}-\mathcal{F}\circ[\mathrm{Tr}(\mathcal{F})]+[d]=[0]$，所以在形式群中 $(c_1^2-c_1\mathrm{Tr}(\mathcal{F})+d)\tau+O(\tau^2)=0$，故 τ 的系数为 0，而 $\pi(\mathcal{F})$ 可分，则 c_1 一定非 0，所以 $\mathrm{Tr}(\mathcal{F})=c_1+\dfrac{d}{c_1}$.

因为 $\hat{\Phi}$ 是 q 次的同种，$\pi(\hat{\Phi})=\hat{\varphi}$ 是可分的，若

$$\hat{\Phi}(\tau)=\tau\circ\hat{\Phi}=\sum_{k\geqslant 1}c_k\tau^k,$$

由上述定理可知

$$\mathrm{Tr}(\hat{\Phi})=c_1+\frac{q}{c_1}.$$

则只需要计算 c_1 即可解决求迹的问题. 其关键是，由于 $\hat{\Phi}$ 是一些同种的复合，所以可以通过计算这些同种在相应的形式群上的表示式中的第一个系数的乘积来得到，即若 $\hat{\Sigma}_i\in\mathcal{E}_{i+1}(\mathbb{Q}_q(\mathcal{E}_i))$ 在形式群上表示为

$$\hat{\Sigma}_i(\tau_i)=g_i\tau_{i+1}+O(\tau_{i+1}^2).$$

则有

$$c_1=\prod_{0\leqslant i<m}g_i;$$

$$\mathrm{Tr}\varphi \equiv \prod_{0\leqslant i<m} g_i \mod q.$$

注意到 g_i 的这个乘积实际上是 g_0 的 $\mathbb{Z}_q$ 到 $\mathbb{Z}_p$ 的范数，故其值一定是 $\mathbb{Z}_p$ 中的元素，另外它给出了精度为 $O(p^m)$ 的 φ 的迹，若需要更高的精度，则必须将 q/c_1 考虑进去.

所以 Frobenius 自同态迹的求取转化为由 $\mathcal{E}_i,\mathcal{E}_{i+1}$ 和 $\hat{\Sigma}_i$ 来计算每个 g_i. 同种 $\hat{\sigma}_i,\hat{\Sigma}_i$ 是 p 次可分的，其核的阶为 p，故由 Vélu 公式知提升 $\hat{\sigma}_i,\hat{\Sigma}_i$ 可通过提升其核得到. 实际上，在已知 $\hat{\Sigma}_i$ 的核的条件下，利用 Vélu 公式 [139]，可将每个 g_i 表示为一些已经获得的提升数据的有理分式，将其相乘即得适当精度的迹. 至此，遗留的问题是如何获得典型提升的曲线方程及 $\hat{\Sigma}_i$ 的核. 当 $p=2$ 或 3 时，可利用 Newton 插值提升单点而提升其核；当 $p\geqslant 5$ 时，可通过更一般的 Hensel 提升，通过提升 p 可除多项式的因式而提升其核. 而第一个问题的解决需要用到模多项式.

模多项式 $\Phi_p(X,Y)$ 是 $p+1$ 次的对称整系数多项式，且若 k 上的椭圆曲线 E,E' 间存在 l 次循环同种，则 $\Phi_l(j(E),j(E'))=0$. 模多项式还满足 Kronecker 关系：

$$\Phi_p(X,Y)\equiv (X^p-Y)(X-Y^p) \mod p.$$

当 p 增大时，其系数会变得非常大，这里仅给出 Φ_2：

$$\begin{aligned}\Phi_2(X,Y)=&X^3+Y^3-X^2Y^2+c_1(XY^2+X^2Y)-c_2(X^2+Y^2)\\&+c_3XY+c_4(X+Y)-c_5,\end{aligned}$$

其中

$$\begin{aligned}c_1&=1488, & c_2&=162000,\\ c_3&=40773375, & c_4&=8748000000,\\ c_5&=157464000000000.\end{aligned}$$

Lubin,Serre 和 Tate[77] 的定理使得可以通过提升 j 不变量将 $\mathbb{F}_q$ 上的椭圆曲线典型提升为 $\mathbb{Z}_q$ 上的曲线 $\mathcal{E}.\mathcal{E}$ 是唯一的保持自同态环不变的 E 的提升.

定理 4.6.17 (Lubin-Serre-Tate) *设 E 是定义在 k 上的椭圆曲线，其 j 不变量 $j\in\mathbb{F}_q\backslash\mathbb{F}_{p^2}$，则存在唯一的 $J\in\mathbb{Z}_q$，使得*

$$\Phi_p(J,\Sigma(J))=0\text{且}J\equiv j \mod p,$$

其中， J 是 E 的典型提升 $\mathcal{E}$(在同构意义下) 的 j 不变量.

综上,可知 Satoh 算法包含两个阶段:以适当的精度提升所需的数据,利用获得的提升数据计算 Frobenius 自同态的迹. 本书介绍的算法利用 k 上的小 Frobenius 映射 σ 构造了 j 不变量圈，基于多变量的 Newton 插值公式将它们同时提升，从而在不需要计算 $\mathbb{Z}_q$ 上的 Σ 的条件下获得了 $\mathbb{Z}_q$ 上的所有共轭 J ，然后利用单变量的 Newton 插值公式通过提升方程的系数求得提升的曲线.

如果 $j(E) \in \mathbb{F}_{p^2}$ ，则可以求得和 E 同构的定义在 $\mathbb{F}_{p^2}$ 上椭圆曲线 E' ，穷举求得 $|E'(\mathbb{F}_{p^2})|$ ，再利用 Weil 定理，便可以求得 $|E'(k)| = |E(k)|$. 故以下均假设 $j(E) \notin \mathbb{F}_{p^2}$.

算法 4.3 (MainAlgorithm)

输入 $\mathbb{F}_q$ 上椭圆曲线 E ， $j(E) \notin \mathbb{F}_{p^2}$.

输出 曲线 E 的阶.

(1) 计算 m 个曲线 E_i 的圈和其相应的 j 不变量 j_i ;

(2) 同时提升所有的 j_i ，获得 J_i ;

(3) 通过提升系数获得所有的曲线;

(4) 提升每条曲线的 p 扭群;

(5) 由以上数据获得 Frobenius 映射的迹，进而求得阶.

上述算法适用于任意特征. 由于 Satoh 算法对于小特征是非常高效的, 而椭圆曲线密码体制的构建中使用的特征为大素数或 2 , 所以以下仅详细讨论 $p = 2, q = 2^m, k = \mathbb{F}_{2^m}$ 的情况.

设定义在 k 上的椭圆曲线 $E : Y^2+XY = X^3+a_2X^2+a_6$, 若 $\mathrm{Tr}(a_2) = 0$, 则通过可允许变换

$$\begin{cases} X \to & X', \\ Y \to & Y' + sX', \end{cases}$$

其中 $s \in k, s^2 + s + a_2 = 0$ ，可得 $E' : Y'^2 + X'Y' = X'^3 + a_6$ ，所以 E 和 E' 同构；若 $\mathrm{Tr}(a_2) = 1$ ，则 E 是 $E' : Y^2 + XY = X^3 + a_6$ 的 a_2 扭曲线，故 $|E(k)| + |E'(k)| = 2q + 2$. 又因为超奇异椭圆曲线不适用于椭圆曲线密码体制的构建，而 j 不变量属于 $\mathbb{F}_4$ 的椭圆曲线的阶有简单的求取方法，故可以仅讨论椭圆曲线

$$E : y^2 + xy = x^3 + a.$$

其中， $j(E) \notin \mathbb{F}_4$ 的求阶问题，即求取 $|E(k)|$.

定理 4.6.18 $4||E(k)|$.

证明 $E(k)$ 中有唯一的 2 阶点 $P=(0,\sqrt{a})$. 设 $x=\sqrt[4]{a}$, 因为 $\mathrm{Tr}\left(x+\dfrac{a}{x^2}\right)=0$, 所以 $Y^2+xY+x^3+a=0$ 在 k 中有根, 记作 y, 则 $Q=(x,y)$ 是 $E(k)$ 的 4 阶点, 所以 $4||E(k)|$.

由 MainAlgorithm 知阶的求取需要提升 j 不变量、提升曲线方程、提升 2 阶点以及 Frobenius 映射迹的计算组成, 下面将分别讨论.

提升 j不变量 Lubin 、 Serre 和 Tate 定理确保了以上构造的 J_i 圈满足 $\Phi_2(J_i,J_{i+1})=0$, 因为 $\Phi_2(j_i,j_{i+1})=0$, $\Phi_2'(j_i,j_{i+1}):=\Phi_2'(X,j_{i+1})|_{j_i}\neq 0$, 所以可以利用 Newton 插值公式以 j_i 为初始值, $k=0$ 来计算 J_i 的近似值, $0\leqslant i<m$, 该插值作用于以下函数:

$$\Theta(x_0,\cdots,x_{m-1})=(\Phi_2(x_0,x_1),\Phi_2(x_1,x_2),\cdots,\Phi_2(x_{m-1},x_0)).$$

Newton 插值算法易于修改为多变量的形式, 其函数求导的过程转换为

$$D\Theta(x_0,\cdots,x_{m-1})=\begin{pmatrix} \Phi_2'(x_0,x_1) & \Phi_2'(x_1,x_0) & 0 & 0\\ 0 & \Phi_2'(x_1,x_2) & \Phi_2'(x_2,x_1) & 0\\ \vdots & \vdots & \vdots & \vdots\\ 0 & 0 & 0 & \Phi_2'(x_{m-1},x_{m-2})\\ \Phi_2'(x_0,x_{m-1}) & 0 & 0 & \Phi_2'(x_{m-1},x_0)\end{pmatrix}$$

其中, $\Phi_2'(X,Y)$ 表示 $\Phi_2(X,Y)$ 相对于 X 的偏导, 其插值公式为

$$(x_0,\cdots,x_{m-1})\leftarrow(x_0,\cdots,x_{m-1})-((D\Theta)^{-1}\Theta)(x_0,\cdots,x_{m-1}).$$

下面详细描述一个算法, 其考虑到每一阶段的精度和上述矩阵的逆. 通过矩阵的行变换可以将左下脚的元素 $\Phi_2'(x_0,x_{m-1})$ 移至右方, 在第 n 步, 它可以被 p^n 整除, 故在所操作的精度内它可以快速为 0 , 则矩阵有一个简单的形式, 可以直接求解.

算法 4.4 (LiftJInvariants)

输入 精度 n, $j_i\in k\backslash\mathbb{F}_4$, 满足 $\Phi_p(j_i,j_{i+1})\equiv 0 \mod 2, 0\leqslant i<m$.

输出 $J_i\in\mathbb{Z}_q$, 满足 $\pi(J_i)=j_i, \Phi_p(J_i,J_{i+1})\equiv 0 \mod 2, 0\leqslant i<m$.

(1) If $n=1$ Then 随机选择 J_i 满足 $\pi(J_i)=j_i$ Goto 5;

(2) $n'\leftarrow\left\lceil\dfrac{n}{2}\right\rceil$;

(3) $(J_0,J_1,\cdots,J_{m-1})\leftarrow$ LiftJInvariants$(n',(j_0,j_1,\cdots,j_{m-1}))$;

(4) $(J_0,J_1,\cdots,J_{m-1})\leftarrow$ UpdateJs$(n,(J_0,J_1,\cdots,J_{m-1}))$;

(5) 返回 $(J_0, J_1, \cdots, J_{m-1})$.

算法 4.5 (UpdateJs)

输入 精度 n 和 $J_i \in \mathbb{Z}_q$, 满足 $\Phi_2(J_i, J_{i+1}) \equiv 0 \mod 2^{\lceil n/2 \rceil}, 0 \leqslant i < m$.

输出 $\mathcal{J}_i \in \mathbb{Z}_q$, 满足 $\Phi_2(\mathcal{J}_i, \mathcal{J}_{i+1}) \equiv 0 \mod 2^n, \mathcal{J}_i \equiv J_i \mod 2^{\lceil n/2 \rceil}, 0 \leqslant i < m$.

(1) 给 $\mathbb{Z}_q$ 中元素 $D[0 \cdots m_2], P[0 \cdots m-1], \mathcal{J}[0 \cdots m-1]$ 分配空间;

(2) For $i = 0$ To $m-2$ Do

$$t \leftarrow 1/\Phi_2'(J_i, J_{i+1});$$

$$D_i \leftarrow t \cdot \Phi_2'(J_{i+1}, J_i);$$

$$P_i \leftarrow t \cdot \Phi_2(J_i, J_{i+1});$$

(3) $m \leftarrow \Phi_2'(J_0, J_{m-1}); f \leftarrow \Phi_2(J_{m-1}, J_0)$;

(4) For $i = 0$ To $m-2$ Do

$$f = f - m \cdot P_i;$$

$$m \leftarrow -m \cdot D_i;$$

$$\text{If } m \equiv 0 \mod 2^n \text{Then Break;}$$

(5) $m \leftarrow m + \Phi_2'(J_{m-1}, J_0)$;

(6) $P_{m-1} \leftarrow f/m$;

(7) For $i = m-2$ Downto 0 Do

$$P_i \leftarrow P_i - D_i \cdot P_{i+1};$$

(8) For $i = 0$ To $m-1$ Do

$$\mathcal{J}_i \leftarrow J_i - P_i;$$

(9) 释放空间 D, P;

(10) 返回 $(\mathcal{J}_0, \mathcal{J}_1, \cdots, \mathcal{J}_{m-1})$.

提升曲线方程 提升曲线方程的算法是利用 Newton 插值通过提升系数 a 来获得提升曲线 $\mathcal{E}$ 的方程 $y^2 + xy = x^3 + A$ 中的系数 A. 因为 $J = \dfrac{1}{\Delta}$, 其中 $\Delta =$

$-A-432A^2$ 是曲线的判别式，所以问题转化为求多项式 $f(x)=1+J(x+432x^2)$ 的根.

因为 $f'(x)=J(1+864x), \pi(J)=j(E)\neq 0$ ，所以可以利用 $k=0$ 的 Newton 插值算法，每一步的精度由 n 转化为 $2n$ ，事实上，可以作稍微的变化，使得精度转化为 $2n+4$. 设 x 是精度为 n 的近似解，则误差 $f(x)=O(2^n)$ ，$y=x-f(x)/f'(x)$ 是每一步改进的解，那么误差变为

$$\begin{aligned} f(y) &= 1+J(y+432y^2) \\ &= 432J\frac{f(x)^2}{f'(x)^2}. \end{aligned}$$

已有 $2\nmid f'(x), 2^4 \| 432$ ，故 $f(y)=O(2^{2n+4})$ ，考虑到效率，初始值最好为 $-1/J \mod 16$.

算法 4.6 (LiftA)

输入 整数 n ，$\mathbb{Z}_q$ 上曲线 $\mathcal{E}$ 的 j 不变量 J ，其精度为 n.

输出 $\mathbb{Z}_q$ 上曲线 $\mathcal{E}$ 的精度为 n 的系数 A.

(1) If $n \leqslant 4$ Then $A \leftarrow -1/J$; Goto 5;

(2) $n' \leftarrow \left\lceil \dfrac{n-4}{2} \right\rceil$;

(3) $A \leftarrow \mathrm{Lift}A(n', J)$;

(4) $A \leftarrow A - \dfrac{1+J(A+432A^2)}{J(1+864A)}$;

(5) 返回 A.

提升 2 阶点 提升 2 阶点的算法也是基于 Newton 插值的. 插值的函数 $f(X)$ 是提升曲线 $\mathcal{E}$ 的 2 阶点所满足的方程，不妨设其为可除多项式 ψ_2 的平方，即 $f(X)=4X^3+X^2+4A$ ，方程 $f(X)=0$ 的任意根 $x\in\mathbb{Z}_q$ 模 2 一定为 0 ，所以可令 $x=2z$ ，便得到修改的多项式 $8X^3+X^2+A$ ，以下对方程 $f(X)=8X^3+X^2+A$ 利用 Newton 插值来求得 z. 显然 $f(X)\equiv 0 \mod 8$ 的根为 $-A$ 模 8 的平方根. 以下记 Z_i 为两倍的 $\hat{\Sigma}_i$ 的核中非平凡点的 X 坐标，亦即 $f(X)=8X^3+X^2+A_i$ 在 $\mathbb{Z}_q$ 中所求得的根. 下面将描述如何确定性地解决该问题.

选择初始值 后面将给出利用 Vélu 公式求取 j 不变量为 J_{i+1} 的曲线 $\mathcal{E}_i'$ ，由 $\mathcal{E}_i'$ 的方程知

$$J_{i+1}=J(\mathcal{E}_i')\equiv\frac{-1}{Z_i^2-Z_i+A_i} \mod 4.$$

因为 Z_i 是 $f(X)$ 的根， $Z_i^2+A_i\equiv 0 \mod 4(8)$ ，则

$$Z_i\equiv\frac{1}{J_{i+1}} \mod 4.$$

该式唯一地确定了 Z_i ，并给出了精度为 2 下的 Newton 插值算法的初始值 Z. 计算得 $f'(X)=2(12X^2+X), 12Z^2+Z\equiv 1/J_{i+1} \mod 4$ ，所以 $f'(Z)\not\equiv 0 \mod 4$ ，则 Newton 插值算法中的 $k=1$. 故为了利用插值算法，必须求得方程 $f(X)$ 模 $2^{2k+1}=8$ 下的根作为插值的初始值. 下证 $f(Z)\equiv 0 \mod 8$. 已有结论 $J_i\equiv-\dfrac{1}{A_i} \mod 8$ ，则

$$\begin{aligned}f(Z)&\equiv Z^2+A_i \mod 8\\&\equiv(1/J_{i+1}^2)+A_i \mod 8\\&\equiv(1/J_{i+1}^2)-(1/J_i) \mod 8.\end{aligned}$$

到此为止，还需要证明 $J_{i+1}^2\equiv J_i \mod 8$. 因为 $J_i=\Sigma(J_{i+1})$ ，所以 $J_{i+1}^2\equiv J_i \mod 2$. 由于 Kronecker 关系在模 16 下也成立, 即 $\Phi_2(X,Y)\equiv(X^2-Y)(X-Y^2) \mod 16$ ，所以

$$\Phi_2(w(j_i),w(j_{i+1}))\equiv 0 \mod 16.$$

又因为 J_{i+1} 的准 Witt 分解中的 x_1,x_2,x_3 均为 0 ，因此 $\Phi_2(J_i,J_{i+1})\equiv 0 \mod 16$ ，故 $J_i\equiv J_{i+1}^2 \mod 16$. 由上知 $Z\equiv 1/J_{i+1} \mod 4$ 是合适的初始值.

提升根 以下利用初始值 $1/J_{i+1} \mod 4$ ， $k=1$ 的 NewtonIterations 算法来计算正确的根 Z_i.

每一步插值将精度由 n 提升为 $2n-1$ ，设 x 是精度为 n 的近似根，其误差 $f(x)=O(2^{n+1})$ ，令 $y=x-f(x)/f'(x)$ 是经过一步插值后改进的根，则新误差为

$$\begin{aligned}f(y)&=8y^3+y^2+A_i\\&=\frac{f(x)^2}{f'(x)^2}(24x+1)-8\frac{f(x)^3}{f'(x)^3}.\end{aligned}$$

因为 $2\|f'(x)$ ，所以 $f(y)=O(2^{\min\{2n,3n+3\}})=O(2^{2n})$.

算法 4.7 (LiftZ)

输入 整数 n ，精度为 2 的 j 不变量 J_{i+1} ，精度为 $n+1$ 的系数 A.

输出 提升曲线 $\mathcal{E}$ 所对应的精度为 n 的 Z.

(1) If $n \leqslant 2$ Then $Z \leftarrow 1/J_{i+1}$; Goto 5;

(2) $n' \leftarrow \left\lceil \dfrac{n+1}{2} \right\rceil$;

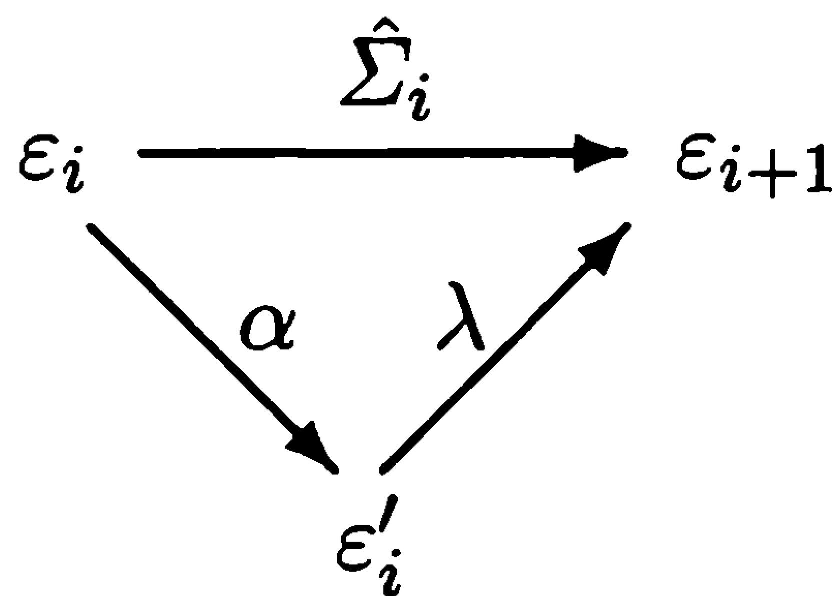
(3) $Z \leftarrow \mathrm{Lift}Z(n', J_{i+1}, A)$;

(4) $Z \leftarrow Z - \dfrac{8Z^3+Z^2+A}{2(12Z^2+Z)}$;

(5) 返回 Z.

Frobenius 映射迹的计算 至此已求得 $\mathcal{E}_i$ 和 $\mathcal{E}_{i+1}$ 两条曲线和 $\mathcal{E}_i$ 的一个 2 阶子群 $C_i = \{(2Z_i, \cdot), O\}$，需要求解的是 $\mathcal{E}_i$ 和 $\mathcal{E}_{i+1}$ 间的同种 $\hat{\Sigma}_i$ 在形式群中表示时的首项系数. 因为 $\hat{\Sigma}_i$ 是 2 次的，$\hat{\Sigma}_i \circ \Sigma_i = 2$，$\mathcal{E}_{i+1}$ 有三个 2 阶点，所以 $\hat{\Sigma}_i$ 的核是由某个 2 阶点生成的 2 阶子群，且在模 2 意义下，该点也属于 $\hat{\sigma}_i$ 的核，则知 $\hat{\sigma}_i$ 的核即为 C_i，故 $\mathcal{E}_{i+1}$ 与 $\mathcal{E}_i/C_i$ 同构. 由 Vélu 公式 [139] 可以求得与 $\mathcal{E}_i/C_i$ 同构的曲线 $\mathcal{E}_i'$ 的方程，以及 $\mathcal{E}_i$ 和 $\mathcal{E}_i'$ 间同种 (称为 Vélu 同种) 的精确公式，而且若将该同种在形式群中表示，其首项系数为 1.

定理 4.6.19 下图是可交换的.



证明 令 $\alpha : \mathcal{E}_i \to \mathcal{E}_i'$ 是 Vélu 构造的同种，则 $\ker\alpha = \ker\hat{\Sigma}_i$，利用文献 [126](推论 III.4.11) 可知存在 $\mathcal{E}_i'$ 到 $\mathcal{E}_{i+1}$ 的同种 λ 使得上图是可交换的. 因为 $\deg(\hat{\Sigma}_i) = \deg(\alpha)\deg(\lambda)$，所以 $\deg(\lambda) = 1$，故 λ 是同构.

由上图的可交换性知同种 $\hat{\Sigma}_i$ 的首项系数 g_i 等于 Vélu 同种的首项系数 (值为 1) 和同构 λ 的首项系数的乘积. 由于 $\mathcal{E}_i'$ 和 $\mathcal{E}_{i+1}$ 的方程已知，所以可以精确地求出同构映射 λ，并获得其形式群表示中的首项系数.

$\mathcal{E}_i$ 的方程为

$$y^2 + xy = x^3 + A_i,$$

$\mathcal{E}_{i+1}$ 的方程为

$$y^2 + xy = x^3 + A_{i+1}.$$

$\hat{\Sigma}_i$ 的核为 $C_i = \{(X_i, Y_i), O\}$ ，显然 $Y_i = -X_i/2$.

Vélu 公式给出的曲线 $\mathcal{E}_i'$ 的方程为 $y^2 + xy = x^3 + \mathcal{A}_4 x + \mathcal{A}_6$ ，其中

$$\mathcal{A}_4 = -5t, \qquad \mathcal{A}_6 = A_i - t - 7w,$$

$$t = 3X_i^2 - Y_i, w = X_i t.$$

已知 $\mathcal{E}_i', \mathcal{E}_{i+1}$ 的方程，可以计算同构及其系数 g_i^2. 通过坐标变换 (不改变同构的形式群表示的首项系数)，方程为

$$\mathcal{E}_{i+1} : y^2 = x^3 - \frac{1}{48}x + \frac{1}{864} + A_{i+1},$$

$$\mathcal{E}_i' : y^2 = x^3 + \left(\mathcal{A}_4 - \frac{1}{48}\right) x + \frac{1}{864} + \mathcal{A}_6 - \frac{\mathcal{A}_4}{12}.$$

则 $\mathcal{E}_i'$ 到 $\mathcal{E}_{i+1}$ 的同构映射 λ 为

$$\lambda : \mathcal{E}_i' \to \mathcal{E}_{i+1}$$

$$(x, y) \mapsto (u^2 x, u^3 y)$$

其中， $u^{-2} = \dfrac{\dfrac{1}{864} + \mathcal{A}_6 - \dfrac{\mathcal{A}_4}{12}}{\dfrac{1}{864} + A_{i+1}} \cdot \dfrac{-\dfrac{1}{48}}{\mathcal{A}_4 - \dfrac{1}{48}}$. 则由 X, Y 的 Laurent 序列 [126], 即 X, Y 相对于 O 点的一致性参数 $\tau = -\dfrac{X}{Y}$ 的表达式

$$X(\tau) = \tau^{-2} - b_1\tau^{-1} - b_2 \cdots$$

$$Y(\tau) = -\tau^{-3} + b_1\tau^{-2} + \cdots,$$

可得

$$\begin{aligned}\lambda(\tau) &= -\frac{u^2 X(\tau)}{u^3 Y(\tau)} = -\frac{u^2\tau^{-2} - u^2 b_1 \tau^{-1} - u^2 b_2 - \dots}{-u^3\tau^{-3} + (u^3 b_1)\tau^{-2} + \dots} \\ &= -\frac{u^2\tau - u^2 b_1 \tau^2 - \dots}{-u^3 + (u^3 b_1)\tau + \dots} = -\frac{u^2(-u^3)}{(-u^3)^2}\tau + O(\tau^2) = \frac{1}{u}\tau + o(\tau^2).\end{aligned}$$

故 $g_i = \dfrac{1}{u}$ ，即

$$g_i^2 = \frac{-\dfrac{1}{48}}{\dfrac{1}{864} + A_{i+1}} \cdot \frac{\dfrac{1}{864} + \mathcal{A}_6 - \dfrac{\mathcal{A}_4}{12}}{\mathcal{A}_4 - \dfrac{1}{48}},$$

简化为

$$g_i^2 = \frac{72\mathcal{A}_4 - 1 + 864\mathcal{A}_6}{(48\mathcal{A}_4 - 1)(1 + 864A_{i+1})}.$$

然后将 $\mathcal{A}_4, \mathcal{A}_6$ 用关于 A_i, X_i 的表达式替换，则

$$g_i^2 = \frac{-18144X_i^3 - 4536X_i^2 - 252X_i + 1 + 864A_i}{(1 + 120X_i + 720X_i^2)(1 + 864A_{i+1})}.$$

因为 $4X_i^3 + X_i^2 + 4A_i = 0$ ，所以上式可简化为

$$g_i^2 = \frac{1 - 252X_i + 19008A_i}{(1 + 120(X_i + 6X_i^2))(1 + 864A_{i+1})}.$$

注意：前面 Newton 插值所求的是 $Z_i = X_i/2$ ，而不是 X_i ，故 Z_i 需要 1 比特的额外精度.

算法 4.8 (ComputeTraceCharTwo)

输入 $\mathbb{F}_{2^m}$ 上椭圆曲线 E,$j(E) \notin \mathbb{F}_4$ ，其方程为 $y^2 + xy = x^3 + a$.

输出 曲线的阶.

(1) $j_0 \leftarrow j(E)$;For $i = m - 1$ Downto 1 Do $j_i \leftarrow j_{i+1}^2$;

(2) $n \leftarrow \left\lceil \frac{m}{2} \right\rceil + 1$;

(3) $(J_i)_{0 \leqslant i < m} \leftarrow$ Lift J Invarianta$(n, (j_i))$;

(4) $N \leftarrow 1; D \leftarrow 1$;

(5) For $i = 0$ To $m - 1$ Do

$A \leftarrow \text{Lift}A(n, J_i)$;

$Z \leftarrow \text{Lift}Z(n-1, J_{i+1}, A)$;

$A \leftarrow 864A$;

$N \leftarrow N(1 - 504Z + 22A)$; ($N$的精度为$n+2$)

$D \leftarrow D(1 + 240(Z + 12Z^2)(1 + A))$;($D$的精度为$n+2$)

(6) $c \leftarrow \sqrt{N/D}$;

(7) If $c \not\equiv 1 \mod 4$ Then $c \leftarrow -c$;

(8) 将 c 约化到 $0 \sim 2^{n+1}$ 间. If $c > 2\sqrt{q}$ Then $c \leftarrow c - 2^{n+1}$;

(9) 返回 $q + 1 - c$.

注意：第 (6) 步中，分母、分子和 c 均是 $\mathbb{Z}_2$ 中的元素， $\sqrt{N/D}$ 通过对其平方根的逆进行 Newton 插值得到. 由定理 4.6.18 知 Frobenius 映射的迹 $\text{Tr}\varphi \equiv 1 \mod 4$ ，所以利用第 (7) 步来选择正确的解.

$\mathbb{F}_q$ 中每个元素所占存储空间为 $O(m)$ 比特，所以 $\mathbb{Z}_q$ 中每个元素需要 $O(m^2)$ 比特的存储空间，该算法涉及 m 个 $\mathbb{Z}_q$ 上的共轭曲线，故总的存储空间为 $O(m^3)$ 比特. 对于任意的 $a \in \mathbb{Z}_q$，存在 $a_0, \cdots, a_{m-1} \in \mathbb{Z}_p$，使得 $a = a_{m-1}t^{m-1} + \cdots + a_0$. $\mathbb{Z}_q$ 中精度为 m 的两个元素相乘可以利用大整数乘法来实现，即通过将每个 a_i 添加适当比特的 0 获得 $\lceil 2m + \log m \rceil$ 比特的大整数，然后将所有的 a_i 对应的大整数黏连起来，得到 $O(m^2)$ 比特的大整数，而两个元素的乘积的相应系数可以从两个黏连而得的大整数的乘积获得. 目前最快速的两个大整数乘法是 Schönhage[115] 提出的，对于 l 比特的两个整数，其计算复杂度为 $O(l \log l \log\log l)$，所以 $\mathbb{Z}_q$ 中精度为 m 的两个元素相乘的计算复杂度为 $O(m^2 \log m \log\log m)$，Newton 插值算法的计算复杂度为 $O(m^2 \log m \log\log m)$，又因为上述算法一共调用了 $O(m)$ 次 Newton 插值算法，所以该算法的时间复杂度为 $O(m^3 \log m \log\log m)$.

定理 4.6.20 设 E 是定义在有限域 k 上的椭圆曲线，且 $j(E) \notin \mathbb{F}_4$，则存在确定性算法求取 $E(k)$ 的阶，其计算复杂度为 $O(m^{3+\varepsilon})$ 次比特运算，其存储空间为 $O(m^3)$ 比特.

实例 以下给出了一个实例的中间结果，有限域为 $\mathbb{F}_{2^{11}} = \mathbb{F}_2[t]/(t^{11} + t^2 + 1)$，其上的椭圆曲线方程为 $E: y^2 + xy = x^3 + a, a = t^4 + t^2 + t$.

首先是提升 j 不变量圈和曲线到精度为 $O(2^7)$，A_i 的结果如下：

$$\begin{aligned}
A_0 &= 30t^{10} + 12t^9 + 30t^8 - 26t^7 - 18t^6 - 12t^5 - 39t^4 - 2t^3 + 41t^2 + 7t - 20,\\
A_1 &= -31t^{10} - 55t^9 - 3t^8 + 43t^7 + 33t^6 + 10t^5 - 50t^4 - 46t^3 + 17t^2 + 20t - 5,\\
A_2 &= -46t^{10} - 53t^9 - 6t^8 + 6t^7 - 18t^6 - 33t^5 + 17t^4 + 31t^3 + 16t^2 - 39t - 15,\\
A_3 &= -8t^{10} - 19t^9 + 47t^8 - 50t^7 - 41t^6 - 14t^5 + 30t^4 + 46t^3 + 9t^2 - 48t - 57,\\
A_4 &= 23t^{10} - 58t^9 - 42t^8 - 26t^7 + 18t^6 + 40t^5 + 29t^4 + 29t^3 - 30t^2 - 38t - 54,\\
A_5 &= 39t^{10} - 43t^9 + 33t^8 - 43t^7 + 30t^6 - 39t^5 - 56t^4 + 34t^3 - t^2 - 27t + 63,\\
A_6 &= 42t^{10} + 31t^9 - 38t^8 + 49t^7 - 49t^6 - 55t^5 - 21t^4 - 42t^3 - 42t^2 + 63t - 51,\\
A_7 &= -62t^{10} - 53t^9 + 46t^8 - 5t^7 - 37t^6 - 26t^5 + 53t^3 + 35t^2 + 52t - 15,\\
A_8 &= 15t^{10} + 54t^9 + 35t^8 - 31t^7 - 58t^6 - 10t^5 + 60t^4 + 49t^3 + 16t^2 + 40t + 26,\\
A_9 &= -58t^{10} + 12t^8 - 45t^8 - 15t^7 - 38t^6 - 63t^5 + 11t^4 + 18t^3 - 8t^2 + 30t - 20,\\
A_{10} &= 56t^{10} + 44t^9 - 57t^8 + 12t^7 + 50t^6 - 54t^5 + 19t^4 - 42t^3 - 53t^2 - 60t - 52.
\end{aligned}$$

$$J_i = \frac{-1}{A_i + 432A_i^2}, \qquad i = 0, 1, \cdots, 10.$$

然后两倍的 2 阶点的 X 坐标被提升到精度为 $O(2^6)$，结果为

$$\begin{aligned}
Z_0 &= -25t^{10}+7t^9-21t^8-3t^7-25t^6+6t^5-2t^4+22t^3-5t^2+32t-11,\\
Z_1 &= 26t^{10}+t^9-30t^8+30t^7-2t^6-7t^5+23t^4+25t^3+28t^2+23t+19,\\
Z_2 &= 32t^{10}-9t^9+9t^8+26t^7+17t^6-30t^5-18t^4-26t^3-9t^2-4t+5,\\
Z_3 &= -23t^{10}+22t^9-2t^8+2t^7-30t^6-16t^5+11t^4+11t^3+10t^2+6t-22,\\
Z_4 &= 13t^{10}+19t^9+7t^8-3t^7+26t^6-25t^5-12t^4+26t^3+25t^2-13t-7,\\
Z_5 &= 10t^{10}+29t^9+18t^8+19t^7-7t^6+3t^5+21t^4-30t^3-2t^2+29t+7,\\
Z_6 &= 22t^{10}+9t^9-22t^8+17t^7-7t^6-26t^5-28t^4-13t^3+5t^2-21,\\
Z_7 &= -23t^{10}+14t^9+5t^8+3t^7-2t^6-14t^5-28t^4-21t^3-12t^2+8t+18,\\
Z_8 &= 14t^{10}+28t^9+17t^8-5t^7-18t^6-25t^5+5t^4-6t^3-24t^2+2t+12,\\
Z_9 &= -16t^{10}-28t^9-3t^8+6t^6-30t^5-15t^4+2t^3+21t^2-28t-28,\\
Z_{10} &= -30t^{10}-28t^9+22t^8-22t^7-22t^6-28t^5-21t^4+10t^3+27t^2+9t-28.
\end{aligned}$$

Frobenius 映射的迹在模 2^9 下的平方数可以通过以下公式计算求得

$$c^2=\frac{\prod_i(1-504Z_i+19008A_i)}{\prod_i(1+240(Z_i+12Z_i^2))(1+864A_i)}\equiv\frac{65}{129}\equiv 449 \mod 2^9.$$

模 2^8 的两个平方根为

$$c\equiv\pm 31 \mod 2^8.$$

选择模 4 同余于 1 的根，即

$$c=-31,$$

则 $|E(\mathbb{F}_{2^{11}})|=2^{11}+1+31=2^{11}+32$.

从以上的讨论可知，在 Satoh 算法中至关重要的是提升 j 不变量和计算 $\hat{\Sigma}_i$ 的核 $\ker(\hat{\Sigma}_i)$. 到目前为止，提升 j 不变量共有 3 种算法. Fouquet 等人 [34] 利用多变量牛顿插值公式在初始值 $x_i\equiv j_i \mod 2$ 下，求得 $\Phi_2(x_0,x_1)=0,\Phi_2(x_1,x_2)=0,\cdots,\Phi_2(x_{m-1},x_0)=0$ 的解 $x_0,x_1,\cdots,x_{m-1}$，由定理 4.6.10 可知 $x_i=J_i,i=0,\cdots,m-1$，其时间复杂度为 $O(m^5)$ 、空间复杂度为 $O(m^3)$;Vercauteren 等人 [140] 证明了如果 $x\equiv J_{i+1} \mod 2^t, y\equiv x^2 \mod 2, \Phi_2(x,y)=0$，则 $y\equiv J_i \mod 2^{t+1}$，他们依据该结论将存储空间减少为 $O(m^2)$;Satoh 等人 [112] 则把以上的结论作了一下改动：如果 $y\equiv J_i \mod 2^t, x\equiv y \mod 2$ 且 $\Phi_2(\Sigma^{-1}(y),x)\equiv 0 \mod 2^{t+1}$，那么 $y\equiv J_i \mod 2^{t+1}$，在此基础上他们提出了一个时间复杂度为

$O(m^{13/3})$ 、空间复杂度为 $O(m^2)$ 的提升算法. 以下依次将它们称为方法一、二、三.

求取 $\hat{\Sigma}_i$ 的核共有两种方法：Fouquet 等人 [34] 利用提升后的 j 不变量求得 $\mathcal{E}_i$ 的方程 $Y^2+XY = X^3+A_i$, 再根据核的性质求解. Skjernaa[130] 在得到提升后的 j 不变量 J_i 后,令 $\mathcal{E}_i$ 的方程为 $Y^2+XY = X^3-36X/(J_i-1728)-1/(J_i-1728)$, 设点 $(2x_i, y_i)$ 是 $\ker(\hat{\Sigma}_i)$ 的非平凡点，则

$$x_i = \frac{(J_{i+1}^2 + 195120J_{i+1} + 4095J_i + 660960000)/2^{12}}{(J_{i+1}^2 + J_{i+1}(563760 - 512J_i) + 8981280000)/2^9}.$$

注意到 $\mathrm{Tr}(\varphi) = \mathrm{Tr}(\hat{\Phi}) \equiv c_0c_1\cdots c_{m-1} \mod q \equiv N_{\mathbb{Q}_q/\mathbb{Q}_2}(c_i) \mod q$, 所以当可以有效求取 2-adic 域上元素的范数时，只需知道一个 c_i 即可求得 Frobenius 映射的迹， Satoh 等人提出的 SST 算法便体现了这一思想. 表 4.1 对 Satoh 系列算法做了比较，有关算法的详细描述可查阅相应的参考文献.

表 4.1 对 Satoh 系列算法做比较

	FGH[34]	Skjernaa[130]	Vercauteren[140]	SST[112]
提升 j 不变量	方法一	方法一	方法二	方法三
$\ker(\hat{\Sigma})$	方法一	方法二	方法二	方法二
$\mathrm{Tr}(\varphi)$	$c_0c_1\cdots c_{n_1}$	$c_0c_1\cdots c_{n-1}$	$c_0c_1\cdots c_{n-1}$	$N_{\mathbb{Q}_q/\mathbb{Q}_p}(c_0)$
时间复杂度	$O(m^{2\varepsilon+1})$	$O(m^{2\varepsilon+1})$	$O(m^{2\varepsilon+1})$	$O(m^{2\varepsilon+1/(\varepsilon+1)})$
空间复杂度	$O(m^3)$	$O(m^3)$	$O(m^2)$	$O(m^2)$

由表 4.1 可知，对于特征为 2 的 Satoh 算法系列而言， SST 算法是目前最有效的算法，这在实际应用中也得到了验证 [112].

4.7 AGM 算法

AGM 算法仅适用于特征为 2 的基域上的椭圆曲线. 它沿用了 Satoh 算法的提升思想，先把有限域上的椭圆曲线和 Frobenius 映射提升到 2-adic 域上，将原椭圆曲线求阶问题转化为求提升 Frobenius 映射的迹，然后利用同种的椭圆曲线的阶相同，构造了一个椭圆曲线簇，依据该簇曲线的性质，把求阶的问题划归为计算 2-adic 域中一个元素的范数，最后构造了一条 AGM 序列来逼近求得所需精度下的范数.

设 $q=2^m, k=\mathbb{F}_q$ ， k 上的椭圆曲线

$$E: Y^2+XY=X^3+\bar{\alpha}^2.$$

其中， $\bar{\alpha}\in k, \bar{\alpha}^2\notin\mathbb{F}_4$. 记 $\mathbb{Z}_q{}^{\times}$ 是 p−adic 整数环 $\mathbb{Z}_q$ 中可逆元的全体.

定理 4.7.1 -1 不是 p 数域 $\mathbb{Q}_q$ 中的平方数.

证明 设 $z\in\mathbb{Q}_q$ 是 -1 的平方根，则 $z\in\mathbb{Z}_q, z^2=-1\equiv 1 \mod 2$. 这说明 $z-1\in 2\mathbb{Z}_q$ ，即 $z=1+c_1 2$ ，其中 $c_1\in\mathbb{Z}_q$ ，但是 $-1\equiv z^2\equiv(1+c_1 2)^2\equiv 1+c_1 4+c_1^2 4\equiv 1 \mod 4$ ，矛盾.

设 $a,b\in\mathbb{Z}_q$ 满足下述条件:

C1 $a,b\in\mathbb{Z}_q^*$;

C2 $a^2\neq b^2$ 且 $ab\neq 0$;

C3 $a,b\equiv 1 \mod 4$;

C4 $a+b\equiv 2 \mod 8$.

对于满足 $x\equiv 1 \mod 8$ 的元素 $x\in\mathbb{Z}_q$ ，$\sqrt{x}$ 均是指满足 $\sqrt{x}\equiv 1 \mod 4$ 的 x 的平方根. 令 $\mathcal{M}(a,b)=\left(\dfrac{a+b}{2},\sqrt{ab}\right),(a_n,b_n)=\mathcal{M}^n(a,b), n\geqslant 1,(a_0,b_0)=(a,b)$.

定理 4.7.2 对于所有的 $n\geqslant 0$ 有:

(1) $a_n,b_n\in\mathbb{Z}_q^*$;

(2) $a_n^2\neq b_n^2$ 且 $a_nb_n\neq 0$;

(3) $a_n,b_n\equiv 1 \mod 4$;

(4) $a_n+b_n\equiv 2 \mod 8$.

证明 $n=0$ 时结论显然成立，假设结论对于 n 成立，即存在 $\alpha,t,t'\in\mathbb{Z}_q$ ，使得

$$a_n=1+4\alpha+8t,\qquad b_n=1-4\alpha+8t',$$

则

$$a_{n+1}=\frac{a_n+b_n}{2}=1+4(t+t'),$$

且

$$b_{n+1}^2=a_nb_n=1+8(t+t')+16(-\alpha^2+2\alpha(t-t')+4tt')\equiv(1+4(t+t'))^2 \mod 16.$$

由推论 4.6.10 知，对于 $n+1$ ，结论 (1) 和 (3) 显然成立. 因为 $\sqrt{a_nb_n}\equiv 1$

mod 4，所以

$$b_{n+1} = \sqrt{a_n b_n} \equiv 1 + 4(t+t') \mod 8,$$

故

$$a_{n+1} + b_{n+1} = \frac{a_n + b_n}{2} + \sqrt{a_n b_n} \equiv 1 + 4(t+t') + 1 + 4(t+t') \equiv 2 \mod 8,$$

即结论 (4) 成立. 进一步结论 (2) 是容易证得的.

定理 4.7.3 假设 $a, b, a', b' \in \mathbb{Z}_q$ 满足 C1~C4，如果存在 $n \geqslant 4$ 使得 $\frac{a}{b} \equiv a'b' \mod 2^n$, 则

$$\frac{\frac{a+b}{2}}{\sqrt{ab}} \equiv \frac{\frac{a'+b'}{2}}{\sqrt{a'b'}} \mod 2^{n+1}.$$

证明 注意到 $ab, \dfrac{a}{b}, a'b', \dfrac{a'}{b'}$ 均有平方根且选择模 4 同余于 1 的平方根. 记

$$\frac{a}{b} = \frac{a'}{b'} + 2^n x,$$

$$\frac{b}{a} = \frac{b'}{a'} + 2^n y.$$

其中，$x \in \mathbb{Z}_q, y = -x\dfrac{bb'}{aa'}$. 因为 $\dfrac{b}{a} \equiv 1 \mod 8, \dfrac{bb'}{aa'} \equiv 1 \mod 2$，所以

$$\begin{aligned}
\frac{\frac{a+b}{2}}{\sqrt{ab}} &= 1/2\left(\sqrt{\frac{a}{b}} + \sqrt{\frac{b}{a}}\right) \\
&= 1/2\left(\sqrt{\frac{a'}{b'}} + 2^{n-1}\frac{x}{\sqrt{\frac{a'}{b'}}} - 2^{2n-3}\frac{x^2}{\left(\frac{a'}{b'}\right)^{3/2}}\right. \\
&\quad \left. + \sqrt{\frac{b'}{a'}} + 2^{n-1}\frac{y}{\sqrt{\frac{b'}{a'}}} - 2^{2n-3}\frac{y^2}{\left(\frac{b'}{a'}\right)^{3/2}} + O(2^{3n-4})\right) \\
&= 1/2\left(\sqrt{\frac{a'}{b'}} + \sqrt{\frac{b'}{a'}} + 2^{n-1}x\sqrt{\frac{b'}{a'}}\left(1 - \frac{b}{a}\right)\right.
\end{aligned}$$

$$-2^{2n-3}x^2\sqrt{\frac{b'}{a'}}\left(\frac{b'}{a'}+\left(\frac{b}{a}\right)^2\right)+O(2^{3n-4})\Bigg)$$

$$=1/2\left(\sqrt{\frac{a'}{b'}}+\sqrt{\frac{b'}{a'}}+O(2^{n+2})\right)$$

$$=\frac{\frac{a'+b'}{2}}{\sqrt{a'b'}}+O(2^{n+1}).$$

对于满足 C1~C4 条件的 $a,b\in\mathbb{Z}_q$，定义 $\mathbb{Z}_q$ 上的曲线 $\mathcal{E}_{a,b}:Y^2=X(X-a^2)(X-b^2)$，容易验证 $\mathcal{E}_{a,b},\mathcal{E}_{\mathcal{M}(a,b)}$ 为椭圆曲线，则有如下结论.

定理 4.7.4 $j(\mathcal{E}_{\mathcal{M}(a,b)})\equiv j(\mathcal{E}_{a,b})^2\mod 2$.

证明 计算得

$$j(\mathcal{E}_{a,b})=\frac{256(a^4-a^2b^2+b^4)^3}{a^4b^4(a^4-2a^2b^2+b^4)},$$

$$j(\mathcal{E}_{\mathcal{M}(a,b)})=\frac{16(14a^2b^2+b^4+a^4)^3}{a^2b^2(6a^4b^4-4b^6a^2-4a^6b^2+b^8+a^8)}.$$

将 $a\equiv 1+4\alpha\mod 8, b\equiv 1-4\alpha\mod 8$ 代入上式有

$$j(\mathcal{E}_{a,b})\equiv 1/\alpha^2\mod 2,$$

$$j(\mathcal{E}_{\mathcal{M}(a,b)})\equiv 1/\alpha^4\mod 2.$$

故结论成立.

令

$$Q_{a,b}:Y^2=X^3+2(a^2+b^2)X^2+(a^2b^2)X,$$

则可以证明 $Q_{a,b}$ 是椭圆曲线，且

$$f:\mathcal{E}_{a,b}\to Q_{a,b},$$
$$(x,y)\mapsto\left(\frac{y^2}{x^2},\frac{y(a^2b^2-x^2)}{x^2}\right)$$

是同种，其对偶同种为

$$\hat{f}:Q_{a,b}\to\mathcal{E}_{a,b},$$
$$(x,y)\mapsto\left(\frac{y^2}{4x^2},\frac{y((a^2-b^2)-x^2)}{8x^2}\right).$$

因为 $f \circ \hat{f} = 2$，而 $f \circ \hat{f} = \deg f$，所以 $\deg f = 2$.

定理 4.7.5 f 的核 $\ker(f) =< (0,0) >\in \mathcal{E}_{a,b}$，$\hat{f}$ 的核 $\ker(\hat{f}) =< (0,0) >\in Q_{a,b}$.

证明 f 的核由 $\frac{Y^2}{X^2}$ 的极点构成. 因为 $\frac{\partial \mathcal{E}_{a,b}}{\partial Y}|_{(0,0)} = 0$，所以 Y 是 $(0,0)$ 点的一致性参数，$(0,0)$ 是 X 的 2 重零点，故 $(0,0)$ 是 $\frac{Y^2}{X^2}$ 的 2 重极点，又因为 X 的有限零点只有 $(0,0)$，而 $(0,0)$ 是 $\mathcal{E}_{a,b}$ 的 2 阶点，所以 $\ker(f) =< (0,0) >= \{(0,0), O\}$. 同理可得 $\ker(\hat{f}) =< (0,0) >$.

定理 4.7.6 有以下同构，

$$
\begin{aligned}
g:\ Q_{a,b} &\to \mathcal{E}_{\mathcal{M}(a,b)},\\
(x,y) &\to \left(\frac{x+(a+b)^2}{4}, -\frac{y}{8}\right).
\end{aligned}
$$

证明 因为 g 是可允许变换，所以 g 是同构.

定理 4.7.7 令 $\phi = g \circ f : \mathcal{E}_{a,b} \to \mathcal{E}_{\mathcal{M}(a,b)}$，则有：

(1) $\ker(\phi) = \{O, (0,0)\}$;

(2) $\ker(\hat{\phi}) = \left\{O, \left(\left(\frac{a+b}{2}\right)^2, 0\right)\right\}$;

(3) $\hat{\phi}(\tau) = \tau + O(\tau^2)$;

(4) $\deg \phi = 2$.

证明 (1) 因为 $\ker(\phi) = \ker(g \circ f)$，由定理 4.7.6 知 $\ker(g \circ f) = \ker(f)$，再利用定理 4.7.5 即得结论.

(2) $\ker(\hat{\phi}) = \ker(\hat{f} \circ \hat{g})$，因为 g 是同构，所以 $g \circ \hat{g} = 1$，故 $\ker(\hat{\phi}) = g(\ker(\hat{f})) = g(\{(0,0), O\}) = \left\{\left(\left(\frac{a+b}{2}\right)^2, 0\right), O\right\}$.

(3) 由文献 [126](p113) 知，X, Y 的 Laurent 序列为 $X(\tau) = \tau^{-2} + \cdots, Y(\tau) = -\tau^{-3} + \cdots$，所以

$$
\begin{aligned}
\hat{f}(\tau) &= \tau \circ \hat{f}\\
&= -\frac{Y^2/(4X^2)}{Y(a^2b^2 - X^2)/(8X^2)}\\
&= -2\frac{Y}{a^2b^2 - X^2}
\end{aligned}
$$

$$
\begin{aligned}
&= -2\frac{-\tau^{-3}+\cdots}{-\tau^{-4}+\cdots}\\
&= -2\tau + O(\tau^2),\\
g(\tau) &= \tau\circ g\\
&= -\frac{\frac{X+(a+b)^2}{4}}{-\frac{Y}{8}}\\
&= 2\frac{X+(a+b)^2}{Y}\\
&= 2\frac{\tau^{-2}+\cdots}{-\tau^{-3}+\cdots}\\
&= -2\tau + O(\tau^2).
\end{aligned}
$$

因为 $g\circ\hat{g}=1$，所以

$$
\tau = (g\circ\hat{g})(\tau) = \tau\circ(g\circ\hat{g}) = (-2\tau+O(\tau^2))\circ\hat{g},
$$

则

$$
\begin{aligned}
&\hat{g}(\tau) = -\frac{1}{2}\tau + O(\tau^2),\\
&\hat{\phi}(\tau) = \tau\circ\hat{\phi} = \tau\circ(\hat{f}\circ\hat{g}) = (-2)\cdot(-\frac{1}{2})\tau + O(\tau^2) = \tau + O(\tau^2).
\end{aligned}
$$

(4) 因为 g 是同构，所以 $\deg g = 1$，已有结论 $\deg f = 2$，故 $\deg\phi = \deg g\deg f = 2$.

提升 j不变量 设 $\alpha\in\mathbb{Z}_q$ 是 $\bar{\alpha}$ 的一个提升，$E/\mathbb{Q}_q$ 表示 E 到 $\mathbb{Q}_q$ 的形如

$$
Y^2+XY=X^3-\alpha^2
$$

的提升.

引理 4.7.8 (1) $E/\mathbb{Q}_q$ 的 2 阶点是 $\mathbb{Q}_q$ 有理点且可以通过下式计算得，即

$$
\begin{aligned}
&(x_1,y_1)\equiv(2\alpha+8\alpha^2,-\alpha+4\alpha^2-8\alpha^3) \mod 16,\\
&(x_2,y_2)\equiv(-2\alpha+8\alpha^2,\alpha+4\alpha^2-8\alpha^3) \mod 16,\\
&(x_3,y_3)=(-1/4+16\alpha^2+O(2^6),1/8+24\alpha^2+O(2^5)).
\end{aligned}
$$

(2) 如果对 $E/\mathbb{Q}_q$ 做以下的可允许变换：

① $u=1,s=1/2,r=t=0$(凑平方);

② $u = 1/2, r = x_3, s = t = 0$(将 (x_3, y_3) 移至 (0,0)),
则得定义在 $\mathbb{Q}_q$ 上的椭圆曲线 $\mathcal{E}_{a,b}$

$$\mathcal{E}_{a,b} : y^2 = x(x - a^2)(x - b^2).$$

其中, $a, b \in \mathbb{Z}_q, a \equiv 1 + 4\alpha + 8\alpha^2 \mod 16, b \equiv 1 - 4\alpha + 8\alpha^2 \mod 16.$

证明 (1) 设 $E/\mathbb{Q}_q$ 的 2 阶点为 (x, y),则有 $2y + x = 0$,设 $x = 2z$,则 $y = -z$,将其代入 $E/\mathbb{Q}_q$ 的方程得

$$0 = 8z^3 + z^2 - \alpha^2,$$

该式模 8 下有解 $\pm\alpha \in \mathbb{Z}_q$,由推论 4.6.8 知该式在 $\mathbb{Z}_q$ 中一定至少有两个解. 以 $\pm\alpha \mod 8$ 为初始,利用 Newton 插值,可得到上式的两个解 $z_1, z_2 \in \mathbb{Z}_q$:

$$z_1 \equiv \alpha + 60\alpha^2 + 40\alpha^3 + 32\alpha^5 \mod 64,$$

$$z_2 \equiv -\alpha + 60\alpha^2 - 40\alpha^3 - 32\alpha^5 \mod 64.$$

那么第三个解 z_3 一定属于 $\mathbb{Q}_q$,并且由

$$8z^3 + z^2 - \alpha^2 = 8(z - z_1)(z - z_2)(z - z_3)$$

可以求得该解:

$$z_3 = -1/8 - z_1 - z_2 = -1/8 + 8\alpha^2 + O(2^6).$$

这意味着 $E/\mathbb{Q}_q$ 的 2 阶点为

$$(x_1, y_1) = (2z_1, -z_1) \equiv (2\alpha + 8\alpha^2, -\alpha + 4\alpha^2 - 8\alpha^3) \mod 16;$$
$$(x_2, y_2) = (2z_2, -z_2) \equiv (-2\alpha + 8\alpha^2, \alpha + 4\alpha^2 - 8\alpha^3) \mod 16;$$
$$(x_3, y_3) = (2z_3, -z_3) = (-1/4 + 16\alpha^2 + O(2^6), 1/8 + 24\alpha^2 + O(2^5)).$$

(2) 对 $E/\mathbb{Q}_q$ 进行两个坐标变换:
① $u = 1, s = 1/2, r = t = 0$;
② $u = 1/2, r = x_3, s = t = 0$.
得下式

$$E' : y^2 = x(x - t_1)(x - t_2),$$

其中，$t_1, t_2 \in \mathbb{Z}_q, t_1 \equiv 1+8\alpha \mod 32, t_2 \equiv 1-8\alpha \mod 32. t_1, t_2$ 均有模 8 为 1 的平方根，由推论 4.6.10 知，t_1, t_2 分别有平方根 $a, b \in \mathbb{Z}_q$，其中 $a \equiv 1+4\alpha+8\alpha^2 \mod 16, b \equiv 1-4\alpha+8\alpha^2 \mod 16$，显然 a, b 满足 C1~C4，故 $\mathcal{E}_{a,b}$ 是可以定义的，显然 $\mathcal{E}_{a,b} = E'$.

定理 4.7.9　设 $g \in \mathbb{Z}_q[X, Y]$, $x_0, y_0 \in \mathbb{Z}_q$ 满足

$$
\begin{aligned}
g(x_0, y_0) &\equiv 0 \mod 2;\\
\frac{\partial g}{\partial X}(x_0, y_0) &\equiv 0 \mod 2;\\
\frac{\partial g}{\partial Y}(x_0, y_0) &\not\equiv 0 \mod 2.
\end{aligned}
$$

则有下述性质：

(1) 对于每一个 $x \in \mathbb{Z}_q, x \equiv x_0 \mod 2$, 存在唯一的 $y \in \mathbb{Z}_q$ 满足 $y \equiv y_0 \mod 2, g(x, y) = 0$;

(2) 设 $x' \in \mathbb{Z}_q, x \equiv x' \mod 2^M, M \geqslant 1, y' \in \mathbb{Z}_q$ 是满足 $y' \equiv y_0 \mod 2, g(x', y') = 0$ 的唯一元素，则 $y' \equiv y \mod 2^{M+1}$.

证明　(1) 定义 $h \in \mathbb{Z}_q[Y], h(Y) = g(x_0, Y)$，则 $h(y_0) \equiv 0 \mod 2, h'(y_0) \equiv \frac{\partial g}{\partial Y}(x_0, y_0) \mod 2$，因此 $h'(y_0) \not\equiv 0 \mod 2$，推论 4.6.8 保证了存在唯一的 $y \in \mathbb{Z}_q$ 满足 $h(y) = g(x_0, y) = 0, y \equiv y_0 \mod 2$. 即对于给定的 x，将 $y_0 \mod 2$ 作为初始值，利用 $g(x_0, Y)$ 上 $k = 0$ 的 Newton 插值可以获得任意精度的 y.

(2) 定义 $\delta_x = x' - x, \delta_y = y' - y$，显然 $\delta_x \equiv \delta_y \equiv 0 \mod 2^M$. 记 $g(X, Y)$ 在 (x, y) 的 Taylor 展开式为 $g(X, Y) = \sum\limits_{i,j} g_{i,j}(X - x)^i (Y - y)^j$，则

$$
\begin{aligned}
0 &= g(x', y')\\
&= g(x + \delta_x, y + \delta_y)\\
&= \sum_{i,j} g_{i,j} \delta_x^i \delta_y^j.
\end{aligned}
$$

其中，$g_{0,0} = g(x, y) = 0, g_{i,j} = \frac{\partial g}{\partial^i X \partial^j Y}(x, y)$，又因为 $\delta_x^2 \equiv \delta_y^2 \equiv 0 \mod 2^{2M}, M \geqslant 1$，所以

$$
0 \equiv \frac{\partial g}{\partial X}(x, y)(x - x') + \frac{\partial g}{\partial Y}(x, y)(y - y') \mod 2^{M+1}.
$$

又因为 $\delta_x \equiv \delta_y \equiv 0 \mod 2^M, \dfrac{\partial g}{\partial Y}(x,y) \not\equiv 0 \mod 2, \dfrac{\partial g}{\partial X}(x,y) \equiv 0 \mod 2$，所以 $y \equiv y' \mod 2^{M+1}$.

该定理给出了一个提升 j 不变量的方法. 设 $a' = 1+4\alpha, b' = 1-4\alpha$，则在模 16 下 $\mathcal{E}_{a',b'}: y^2 = x(x-a'^2)(x-b'^2)$ 与 $\mathcal{E}_{a,b}$ 相同，所以 $\mathcal{E}_{a',b'}$ 在同构意义下也模 2 约化为 E.

推论 4.7.10 $j(\mathcal{E}_{\mathcal{M}^n(a',b')}) \equiv j(\mathcal{E}^{\Sigma^n}) \mod 2^{n+1}\ \forall n \geqslant 0$.

证明 当 $n=0$ 时，因为 $\mathcal{E}_{a',b'}$ 在同构意义下也模 2 约化为 E，所以 $j(\mathcal{E}_{a',b'}) \equiv j(\mathcal{E}) \mod 2$. 假设结论对 n 成立.

令 $x_0 = j(\mathcal{E}_{a_n,b_n}), y_0 = j(\mathcal{E}_{\mathcal{M}(a_n,b_n)}), x' = j(\mathcal{E}_{a'_n,b'_n}), y' = j(\mathcal{E}_{\mathcal{M}(a'_n,b'_n)})$, $x = j(\mathcal{E}^{\Sigma^n}), y = j(\mathcal{E}^{\Sigma^{n+1}})$，由归纳假设知 $x' \equiv x \mod 2^{n+1}$，要证 $y' \equiv y \mod 2^{n+2}$.

因为 $\phi: \mathcal{E}_{a_n,b_n} \to \mathcal{E}_{\mathcal{M}(a_n,b_n)}$ 的次数为 2，所以 $\Phi_2(x_0,y_0) = 0$. 已知 $j(\mathcal{E}_{a,b}) = j(\mathcal{E})$，$j(E) \notin \mathbb{F}_4$，所以 $j(\mathcal{E}_{a,b}) \mod 2 \notin \mathbb{F}_4, x_0 \equiv j(\mathcal{E}_{a,b})^{2n} \mod 2 \notin \mathbb{F}_4$，故由定理 4.7.4 知

$$\begin{aligned}
\frac{\partial \Phi_2}{\partial X}(x_0,y_0) &\equiv j(\mathcal{E}_{a_n,b_n})^2 - j(\mathcal{E}_{\mathcal{M}(a_n,b_n)}) \mod 2 \\
&\equiv j(\mathcal{E}_{a_n,b_n})^2 - j(\mathcal{E}_{a_n,b_n})^2 \mod 2 \\
&\equiv 0 \mod 2, \\
\frac{\partial \Phi_2}{\partial Y}(x_0,y_0) &\equiv j(\mathcal{E}_{a_n,b_n}) - j(\mathcal{E}_{\mathcal{M}(a_n,b_n)})^2 \mod 2 \\
&\equiv j(\mathcal{E}_{a_n,b_n}) - j(\mathcal{E}_{a_n,b_n})^4 \mod 2 \\
&\not\equiv 0 \mod 2.
\end{aligned}$$

因为 $x \equiv j(\mathcal{E})^{2n} \mod 2$，所以 $x \equiv x_0 \mod 2$，$y \equiv y_0 \mod 2$. 而 $\mathcal{E}^{\Sigma^n}$ 与 $\mathcal{E}^{\Sigma^{n+1}}$ 间存在小 Frobenius 映射，故 $\Phi_2(x,y) = 0$. 归纳假设为 $x \equiv x' \mod 2^{n+1}$，则 $y \equiv x^2 \equiv x'^2 \equiv y' \mod 2$. 又因为 $\phi: \mathcal{E}_{a'_n,b'_n} \to \mathcal{E}_{\mathcal{M}(a'_n,b'_n)}$ 的次数为 2，所以 $\Phi_2(x',y') = 0$. 以上说明满足定理 4.7.9 的条件，故有结论

$$j(\mathcal{E}_{\mathcal{M}(a'_n,b'_n)}) \equiv j(\mathcal{E}^{\Sigma^{n+1}}) \mod 2^{n+2}.$$

由该推论知，$j(\mathcal{E}_{a'_m,b'_m}) \equiv j(\mathcal{E}^{\Sigma^m}) \equiv j(\mathcal{E}) \mod 2^{m+1}$，即通过求取 a'_m, b'_m 便可以得到 E 的提升的 j 不变量.

求取 $\hat{\Sigma}$的核

引理 4.7.11 $j(\mathcal{E})\in\mathbb{Z}_q$ 是平方数.

证明 已有结论 $j(\mathcal{E}_{a,b})\equiv j(\mathcal{E}) \mod 2$，再利用定理 4.7.9 可知 $j(\mathcal{E}_{\mathcal{M}^2(a,b)})\equiv j(\mathcal{E}^{\Sigma^2}) \mod 8$. 由 $a\equiv 1+4\alpha+8\alpha^2 \mod 16, b\equiv 1-4\alpha+8\alpha^2 \mod 16$ 计算得

$$j(\mathcal{E}_{\mathcal{M}^2(a,b)})=\frac{2^8(1+O(8))^3}{2^{24}(\alpha^8+O(8))}\equiv 1/\alpha^8 \mod 8.$$

所以 $j(\mathcal{E}_{\mathcal{M}^2(a,b)}), j(\mathcal{E}^{\Sigma^2})$ 是模 8 的平方数，由推论 4.6.10 知它们在 $\mathbb{Z}_q$ 中也是平方数，因为 $\mathcal{E}=(\mathcal{E}^{\Sigma^{m-2}})^{\Sigma^2}$，故 $j(\mathcal{E})$ 是 $\mathbb{Z}_q$ 中的平方数.

推论 4.7.12 存在 $\alpha\in\mathbb{Z}_q{}^*$，使得 $\mathcal{E}$ 的方程为

$$Y^2+XY=X^3-\alpha^2.$$

证明 注意到对于 $T\in\mathbb{Q}_q$, 若 $T^2-432T^4\neq 0$，则有 $j(Y^2+XY=X^3-T^2)=\dfrac{-1}{T^2(-1+432T^2)}$. 观察多项式

$$f(T)=T^2(-1+432T^2)j(\mathcal{E})+1,$$
$$f'(T)=2T(-1+432T^2)j(\mathcal{E})+864T^3j(\mathcal{E}).$$

由上述引理知 $j(\mathcal{E})$ 是平方数，所以存在 $A=\dfrac{1}{\sqrt{j(\mathcal{E})}}\in\mathbb{Z}_q{}^*$，则 $f(A)\equiv 0 \mod 8, f'(A)\equiv 0 \mod 2, f'(A)\not\equiv 0 \mod 4$，由 Newton 插值知 f 有根 $\alpha\in\mathbb{Z}_q$，即存在定义在 $\mathbb{Z}_q$ 上的椭圆曲线 $\mathcal{E}': Y^2+XY=X^3-\alpha^2$，且 $j(\mathcal{E}')=j(\mathcal{E})$，所以 $\mathcal{E}'$ 与 $\mathcal{E}$ 同构，即 $\mathcal{E}'$ 是 E 到 $\mathbb{Q}_q$ 的典型提升.

以下均假设 α 为推论 4.7.12 中所给出的值.

推论 4.7.13 可以找到 $a,b\in\mathbb{Z}_q$ 以及一个定义在 $\mathbb{Q}_q$ 上的可允许坐标变换将 $\mathcal{E}$ 变换为 $\mathcal{E}_{a,b}$，满足如下条件:

(1) $\mathcal{E}_{a,b}: Y^2=X(X-a^2)(X-b^2), a\equiv 1+4\alpha+8\alpha^2 \mod 16, b\equiv 1-4\alpha+8\alpha^2 \mod 16$;

(2) $\ker(\Sigma:\mathcal{E}_{a,b}\to\mathcal{E}_{a,b}^{\Sigma})=\{(0,0),O\}$;

(3) $\ker(\hat{\Sigma}:\mathcal{E}_{a,b}^{\Sigma}\to\mathcal{E}_{a,b})=\{(\Sigma(a^2),0),O\}$.

证明 $\mathcal{E}$ 满足引理 4.7.8 的条件，所以存在 $a,b\in\mathbb{Z}_q$ 和可允许变换将 $\mathcal{E}$ 变换为 $\mathcal{E}_{a,b}$，其中

$$a \equiv 1 + 4\alpha + 8\alpha^2 \mod 16;$$
$$b \equiv 1 - 4\alpha + 8\alpha^2 \mod 16.$$

Σ 次数为 2 ，且其核由某个 2 阶点生成. 因为 $\hat{\Sigma} \circ \Sigma = 2$ ，而 $\mathcal{E}_{a,b}$ 中有 3 个 2 阶点，所以 $|\ker(\hat{\Sigma} \circ \Sigma)| = 4$ ，又因为 $\hat{\Sigma}, \Sigma$ 的次数均为 2 ，所以 $|\ker \hat{\Sigma}| = |\ker \Sigma| = 2$ ，它们的核是由 2 阶点生成的 2 阶群. σ 是单映射，引理 4.7.8 中的 2 阶点 $(x_1, y_1), (x_2, y_2)$ 模 2 相等，不为 O ，所以 $(x_1, y_1), (x_2, y_2)$ 对应的 $\mathcal{E}_{a,b}$ 中的点不是 Σ 的核，故

$$\ker(\Sigma) = \{(0,0), O\}.$$

因为 $(a^2, 0), (\Sigma(a^2), 0)$ 分别是 $\mathcal{E}_{a,b}, \mathcal{E}_{a,b}^{\Sigma}$ 的 2 阶点，所以

$$\hat{\Sigma}((\Sigma(a^2), 0)) = \hat{\Sigma} \circ \Sigma((a^2, 0)) = 2((a^2, 0)) = O,$$
$$\ker(\hat{\Sigma}) = \{(\Sigma(a^2), 0), O\}.$$

以下假设 a, b 即是该推论中所定义的值，这意味着 $\mathcal{E}_{a,b} : Y^2 = X(X - a^2)(X - b^2)$ 是 E 的典型提升. 因为

$$\phi : \mathcal{E}_{a,b} \to \mathcal{E}_{\mathcal{M}(a,b)}$$

是可分的，且 $\ker(\phi) \subseteq \ker(\Sigma)$ ，所以由文献 [126](corr 4.11) 知存在唯一的同种，即

$$\lambda : \mathcal{E}_{\mathcal{M}(a,b)} \to \mathcal{E}_{a,b}^{\Sigma},$$

满足 $\Sigma = \lambda \circ \phi$.

引理 4.7.14 $\lambda : (x, y) \mapsto (u^2 x, u^3 y)$ 是 $\mathcal{E}_{\mathcal{M}(a,b)}$ 到 $\mathcal{E}_{a,b}^{\Sigma}$ 的同构，其中 $u \in \mathbb{Q}_q$ ， $u = \pm \dfrac{\Sigma a}{\dfrac{a+b}{2}}$.

证明 因为 $\deg \Sigma = 2, \deg \phi = 2$ ，所以

$$2 = \deg \Sigma = \deg \lambda \deg \phi = \deg \lambda \cdot 2,$$

即 $\deg \lambda = 1$ ，所以 λ 是同构. 设

$$\lambda : (x, y) \mapsto (u^2 x + r, u^3 y + s u^2 x + t),$$

其中， u, r, s, t 属于 $\mathbb{Q}_q$ 的代数闭域，则

$$X = u^2X' + r;$$
$$Y = u^3Y' + su^2X' + t.$$

是 $\mathcal{E}_{a,b}^{\Sigma}$ 到 $\mathcal{E}_{\mathcal{M}(a,b)}$ 的可允许坐标变换，比较系数即得 $s = t = 0$.

因为同构的椭圆曲线 $\mathcal{E}_{a,b}^{\Sigma}, \mathcal{E}_{\mathcal{M}(a,b)}$ 上的 2 阶点组成的群分别为

$$\{O, (0,0), (\Sigma(a^2), 0), (\Sigma(b^2), 0)\},$$

$$\left\{O, (0,0), \left(\left(\frac{a+b}{2}\right)^2, 0\right), (ab, 0)\right\},$$

故

$$\left\{\lambda(0,0), \lambda\left(\left(\frac{a+b}{2}\right)^2, 0\right), \lambda(ab, 0)\right\} \subseteq \{(0,0), (\Sigma(a^2), 0), (\Sigma(b^2), 0)\}$$

且互不相同, 则 $r \in \{0, \Sigma(a^2), \Sigma(b^2)\}$. 假设 $r = \Sigma(a^2)$, 则 $0 = u^2\left(\frac{a+b}{2}\right)^2 + \Sigma(a^2)$ 或 $0 = u^2ab + \Sigma(a^2)$ ，故 $-1 = \left(\frac{u\left(\frac{a+b}{2}\right)}{\Sigma a}\right)^2$ 或 $-1 = \left(\frac{u\sqrt{ab}}{\Sigma a}\right)^2$.
由定理 4.7.1 知 -1 不是 $\mathbb{Q}_q$ 中的平方数，矛盾，因此 $r \neq \Sigma(a^2)$ ；同理可证得 $r \neq \Sigma(b^2)$ ；故 $r = 0$.

因为

$$\ker(\hat{\Sigma} : \mathcal{E}_{a,b}^{\Sigma} \to \mathcal{E}_{a,b}) = \lambda(\ker\hat{\phi}) = \{(\Sigma(a^2), 0), O\},$$

而 $\ker\hat{\phi} = \left\{\left(\left(\frac{a+b}{2}\right)^2, 0\right), O\right\}$ ，所以

$$\lambda\left(\left(\frac{a+b}{2}\right)^2, 0\right) = (\Sigma(a^2), 0),$$

计算得 $u = \pm\frac{\Sigma a}{\frac{a+b}{2}}$.

将 Σ^{-1} 作用于 λ^{-1} 的坐标函数可得同构

$$\Sigma^{-1}(\lambda^{-1}):\mathcal{E}_{a,b}\to\mathcal{E}_{\mathcal{M}(a,b)}^{\Sigma^{-1}}.$$

故在同构意义下，$\mathcal{E}_{\mathcal{M}(a,b)}^{\Sigma^{-1}}$ 是 E 到 $\mathbb{Q}_q$ 的典型提升. 令

$$\begin{aligned}\Psi_1=\Sigma^{-1}(\lambda^{-1})\circ\hat{\Sigma}\circ\lambda\quad &:\quad \mathcal{E}_{\mathcal{M}(a,b)}\to\mathcal{E}_{\mathcal{M}(a,b)}^{\Sigma^{-1}};\\ \Psi_2=\Sigma(\Psi_1)\quad &:\quad \mathcal{E}_{\mathcal{M}(a,b)}^{\Sigma}\to\mathcal{E}_{\mathcal{M}(a,b)}.\end{aligned}$$

因为同种 $\hat{\Sigma}$ 的次数为 2，所以 Ψ_1,Ψ_2 的次数均为 2. 引理 4.7.14 说明 $\mathcal{E}_{\mathcal{M}(a,b)}$ 和 $\mathcal{E}_{a,b}^{\Sigma}$ 同构，$\mathcal{E}_{a,b}$ 是 E 到 $\mathbb{Q}_q$ 的典型提升，故在同构意义下，$\mathcal{E}_{\mathcal{M}(a,b)},\mathcal{E}_{\mathcal{M}(a,b)}^{\Sigma}$ 是 E^{σ},E^{σ^2} 到 $\mathbb{Q}_q$ 的典型提升，故不考虑正、负号，则 Ψ_1,Ψ_2 是小 Frobenius 映射的提升的对偶同种，以下将其统记为 $\hat{\Sigma}$. 将 $\mathcal{M}(a,b)$ 作为 (a,b)，同上可以知道在同构意义下，$\mathcal{E}_{\mathcal{M}^2(a,b)},\mathcal{E}_{\mathcal{M}^2(a,b)}^{\Sigma}$ 是 $E^{\sigma^2},E^{\sigma^3}$ 的典型提升，一般地有 $\mathcal{E}_{a_i,b_i},\mathcal{E}_{a_i,b_i}^{\Sigma}$ 是 $E^{\sigma^i},E^{\sigma^{i+1}}$ 的典型提升，$i\geqslant 0$.

引理 4.7.15 $\ker(\hat{\Sigma}:\mathcal{E}_{\mathcal{M}(a,b)}^{\Sigma}\to\mathcal{E}_{\mathcal{M}(a,b)})=\{(\Sigma(a_1^2),0),O\}$.

证明 因为 $\Sigma=\lambda\circ\phi$，所以

$$\Sigma^{-1}(\lambda)\circ\Psi_1=\hat{\Sigma}\circ\lambda=\hat{\phi}\circ\hat{\lambda}\circ\lambda=\hat{\phi},$$

故有以下形式：

$$\begin{array}{ccc}\mathcal{E}_{\mathcal{M}(a,b)} & \xrightarrow{\Psi_1} & \mathcal{E}_{\mathcal{M}(a,b)}^{\Sigma^{-1}}\\ \Big\downarrow\hat{\phi} & \simeq & \swarrow\Sigma^{-1}(\lambda)\\ \mathcal{E}_{a,b} & & \end{array}$$

因此有

$$\begin{aligned}&\ker(\Psi_1)=\ker(\hat{\phi})=\{(a_1^2,0),O\},\\ &\ker(\Psi_2)=\ker(\Sigma(\Psi_1))=\{(\Sigma(a_1^2),0),O\},\\ &\ker(\hat{\Sigma}:\mathcal{E}_{\mathcal{M}(a,b)}^{\Sigma}\to\mathcal{E}_{\mathcal{M}(a,b)})=\ker(\Psi_2)=\{(\Sigma a_1^2,0),O\}.\end{aligned}$$

推论 4.7.16 对于任意的 $n\geqslant 1$，有 $\ker(\hat{\Sigma}:\mathcal{E}_{a_n,b_n}^{\Sigma}\to\mathcal{E}_{a_n,b_n})=\{(\Sigma(a_n^2),0),O\}$.

证明 $\mathcal{E}_{a_{n-1},b_{n-1}}$ 是 $E^{\sigma^{n-1}}$ 的典型提升，将引理 4.7.15 中的 (a,b) 用 (a_{n-1}, b_{n-1}) 替换即得结论.

计算 Frobenius 自同态的迹

推论 4.7.17 对于 $\hat{\Sigma}:\mathcal{E}_{a,b}^{\Sigma}\to\mathcal{E}_{a,b}$，有 $\hat{\Sigma}(\tau)=\tau\circ(\hat{\Sigma})=\pm\dfrac{\Sigma a}{\left(\dfrac{a+b}{2}\right)}\tau+O(\tau^2)$.

证明 因为 $\hat{\Sigma}=\hat{\phi}\circ\lambda^{-1}$，所以 $\tau\circ\hat{\Sigma}=\tau\circ(\hat{\phi}\circ\lambda^{-1})$，由定理 4.7.7 知 $\tau\circ\hat{\phi}=\tau+O(\tau^2)$，故

$$\tau\circ\hat{\Sigma}=\tau\circ\lambda^{-1}+O(\tau^2)=\tau+O(\tau^2).$$

结论得证.

令 $\Phi:\mathcal{E}_{a,b}\to\mathcal{E}_{a,b}$ 表示 $\varphi:E\to E$ 的提升.

定理 4.7.18 $\tau\circ\Phi=c_1\tau+O(\tau^2)$，其中 $c_1=\pm N_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\dfrac{a}{\left(\dfrac{a+b}{2}\right)}\right)$.

证明 有如下形式:

$$\begin{array}{ccccccccc}
\mathcal{E}_{a,b} & \xrightarrow{\Sigma} & \mathcal{E}_{a,b}^{\Sigma} & \xrightarrow{\Sigma} & \mathcal{E}_{a,b}^{\Sigma^2} & \xrightarrow{\Sigma} & \cdots & \xrightarrow{\Sigma} & \mathcal{E}_{a,b}^{\Sigma^m}\\
\downarrow & & \downarrow & & \downarrow & & \downarrow & & \downarrow\\
E & \xrightarrow{\sigma} & E^{\sigma} & \xrightarrow{\sigma} & E^{\sigma^2} & \xrightarrow{\sigma} & \cdots & \xrightarrow{\sigma} & E^{\sigma^m}
\end{array}$$

由推论 4.7.17 知

$$\tau\circ(\hat{\Sigma}:\mathcal{E}_{a,b}^{\Sigma^i}\to\mathcal{E}_{a,b}^{\Sigma^{i-1}})=\pm\Sigma^{i-1}\left(\frac{\Sigma a}{\left(\dfrac{a+b}{2}\right)}\right)\tau+O(\tau^2),$$

因此

$$\begin{aligned}
c_1&=\pm\prod_{i=1}^{m}\Sigma^{i-1}\left(\frac{\Sigma a}{\left(\dfrac{a+b}{2}\right)}\right)=\pm\prod_{i=0}^{m-1}\Sigma^{i}\left(\frac{a}{\left(\dfrac{a+b}{2}\right)}\right)\\
&=\pm N_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\frac{a}{\left(\dfrac{a+b}{2}\right)}\right).
\end{aligned}$$

推论 4.7.19 $\operatorname{Tr}(\varphi) \equiv \pm N_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\dfrac{a}{\left(\dfrac{a+b}{2}\right)}\right) \mod 2^m.$

证明 因为 $c_1 \in \mathbb{Z}_q$ 是可逆元，所以

$$\begin{aligned}\operatorname{Tr}(\varphi) &= \operatorname{Tr}(\hat{\varphi}) \\ &= \operatorname{Tr}(\hat{\Phi}) \\ &= c_1 + 2^m/c_1 \\ &\equiv \pm N_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\dfrac{a}{\left(\dfrac{a+b}{2}\right)}\right) \mod 2^m.\end{aligned}$$

算法 4.9

输入 椭圆曲线 $E: Y^2 + XY = X^3 - \bar{\alpha}^2$，其中 $\bar{\alpha} \in \mathbb{F}_{2^m}, \bar{\alpha}^2 \notin \mathbb{F}_4$，且 $\alpha \in \mathbb{Z}_q$ 是 $\bar{\alpha}$ 的提升.

输出 Frobenius 的迹 $t = 2^m + 1 - |E(k)|$.

(1) 令 $a = 1 + 4\alpha, b = 1 - 4\alpha, N = \lceil m/2 \rceil$.

(2) For n from 1 to $N-1$ do

$$(a, b) = \left(\frac{a+b}{2} \mod 2^{n+4}, \sqrt{ab} \mod 2^{n+4}\right).$$

(3) $t = N_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\dfrac{a}{\left(\frac{a+b}{2}\right)}\right) \mod 2^{N+2} \geqslant 0$.

(4) If $t > 2\sqrt{2^d}$ then $t = t - 2^{N+2}$.

(5) If $t \equiv -1 \mod 4$ then $t = -t$.

令 $N = \lceil m/2 \rceil, t = \operatorname{Tr}(\varphi : E \to E)$. 由推论 4.7.12 和推论 4.7.13 知，存在 $A, a, b \in R$ 使得

$$\mathcal{E}_{a,b} : y^2 = x(x - a^2)(x - b^2)$$

是 E 的典型提升，其中

$$\begin{aligned}A &\equiv \alpha \mod 2; \\ a &\equiv 1 + 4\alpha + 8\alpha^2 \mod 16; \\ b &\equiv 1 - 4\alpha + 8\alpha^2 \mod 16.\end{aligned}$$

因为 $\mathcal{E}_{\mathcal{M}^{N-1}(a,b)}$ 是 $E^{\sigma^{N-1}}$ 的典型提升，且 $|E(k)| = |E^{\sigma^{N-1}}|$，所以再利用推论 4.7.16 和推论 4.7.19 知

$$t \equiv \pm N_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\frac{a_{N-1}}{\frac{a_{N-1}+b_{N-1}}{2}}\right) \mod 2^{N+2}.$$

定义

$$a'_0 = 1 + 4\alpha,$$

$$b'_0 = 1 - 4\alpha,$$

$$a'_n = \frac{a'_{n-1} + b'_{n-1}}{2} \mod 2^{n+4},$$

$$b'_n = \sqrt{a'_{n-1}b'_{n-1}} \mod 2^{n+4}.$$

则有以下结论.

引理 4.7.20 $\frac{a_n}{b_n} \equiv \frac{a'_n}{b'_n} \mod 2^{n+4}$.

证明 当 $n = 0$ 时，有

$$\frac{a_0}{b_0} \equiv \frac{1+4A+8A^2}{1-4A+8A^2} \mod 2^4;$$

$$\frac{a'_0}{b'_0} = \frac{1+4\alpha}{1-4\alpha}.$$

因为 $A \equiv \alpha \mod 2$，所以

$$\begin{aligned}&(1+4A+8A^2)(1-4\alpha) - (1-4A+8A^2)(1+4\alpha)\\=&-8(\alpha+A) - 64A^2\alpha\\\equiv&\ 0 \mod 2^4.\end{aligned}$$

至此证明了 $n = 0$ 时结论成立.

假设 $\frac{a_n}{b_n} \equiv \frac{a'_n}{b'_n} \mod 2^{n+4}$，则利用定理 4.7.3 有

$$\frac{a_{n+1}}{b_{n+1}} \equiv \frac{\frac{a'_n+b'_n}{2}}{\sqrt{a'_nb'_n}} \equiv \frac{a'_{n+1}}{b'_{n+1}} \mod 2^{n+1+4}.$$

即结论对于 $n+1$ 也成立. 至此, 结论证毕.

引理 4.7.21 $\dfrac{a_{N-1}}{\dfrac{a_{N-1}+b_{N-1}}{2}} \equiv \dfrac{a'_{N-1}}{\dfrac{a'_{N-1}+b'_{N-1}}{2}} \mod 2^{N+2}$.

证明

$$\begin{aligned}
\frac{a_{N-1}}{\dfrac{a_{N-1}+b_{N-1}}{2}} &= \frac{2}{1+\dfrac{b_{N-1}}{a_{N-1}}} \\
&= \frac{2}{1+\dfrac{b'_{N-1}}{a'_{N-1}}+O(2^{N+3})} \\
&= \frac{2}{1+\dfrac{b'_{N-1}}{a'_{N-1}}}+\frac{1}{2}O(2^{N+3}) \\
&\equiv \frac{a'_{N-1}}{\dfrac{a'_{N-1}+b'_{N-1}}{2}} \mod 2^{N+2}.
\end{aligned}$$

令 $z=\dfrac{a'_{N-1}}{\dfrac{a'_{N-1}+b'_{N-1}}{2}} \mod 2^{N+2}$, 则由引理 4.7.21 知

$$\pm t \equiv N_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\frac{a_{N-1}}{\dfrac{a_{N-1}+b_{N-1}}{2}}\right) \equiv N_{\mathbb{Q}_q/\mathbb{Q}_2}(z) \mod 2^{N+2}.$$

再利用 $|t| \leqslant 2\sqrt{q}$, $t\equiv 1 \mod 4$, 即算法的 (3)~(5) 步便确定了 t. 至此, 说明算法的正确性.

文献 [112] 给出了存储空间为 $O(m^2)$ 比特, 时间复杂度为 $O(m^{2\nu+0.5})$ 次比特运算的算法, 以求取精度为 $\left\lceil \dfrac{m}{2} \right\rceil$ 左右的 $\mathbb{Q}_q$ 上元素的范数, 而 $\mathbb{Z}_q$ 上精度不大于 m 的元素需要的存储空间为 $O(m^2)$ 比特, 每个精度不大于 m 的两个元素的乘法的时间复杂度为 $O(m^2\log m\log\log m)$ 次比特运算, 所以算法的存储空间为 $O(m^2)$ 比特, 时间复杂度为 $O(m^{4.5}\log m\log\log m)$ 次比特运算.

实例 令 $f=X^7+X+1, \mathbb{F}_{2^7}=\mathbb{F}_2[X]/(f), c=X+(f)$. 椭圆曲线为

$$E: y^2+xy=x^3+\frac{1}{c^5+c+1},$$

可以求得 $\alpha = \dfrac{1}{c^6+c^4+c^3+c+1}$. 因此

$$a = 13 + 4c^5 + 8c^3 + 8c^4,$$
$$b = 5 + 12c^5 + 8c^3 + 8c^4,$$

利用 Newton 插值可以求得表 4.2.

表 4.2 利用 Newton 插值求解

n	(a'_n, b'_n)
0	$4c^5+5$
	$12c^5+13$
1	$8c^5+9$
	$24c^5+8c^4+8c^3+1$
2	$16c^5+4c^4+4c^3+5$
	$24c^6+16c^5+52c^4+52c^3+40c^2+24c+13$
3	$12c^6+16c^5+28c^4+28c^3+20c^2+12c+9$
	$36c^6+120c^5+84c^4+108c^3+44c^2+92c+17$

则

$$\frac{a'_3}{\dfrac{a'_3+b'_3}{2}} \mod 2^6 = 52c^6+60c^5+52c^4+40c^3+52c^2+8c+29,$$

计算得

$$N_{\mathbb{Q}_q/\mathbb{Q}_2}\left(\frac{a'_3}{\dfrac{a'_3+b'_3}{2}}\right) \mod 2^6 = 61.$$

最终得 $t=-3, |E(\mathbb{F}_{2^7})| = 2^7+1-t = 132$.

随着 q 的增大， SST 算法会逐渐优于 AGM 算法 (其优势与复杂度前的常数有关). 但值得注意的是， AGM 算法的计算复杂度前的常数非常小，所以在目前密码应用所需的尺寸下，其运行时间少于 SST 算法. SST 算法与 AGM 算法相比，还有一个缺点便是它需要预计算，这使得 SST 算法不能在智能卡上实现. MSST 算法结合了 AGM 算法和 SST 算法. 它首先利用椭圆曲线的同构，将双参数的 AGM 算法改为单参数的 AGM 算法，然后再依据 SST 算法中提升的思想，改进了 AGM 算法中计算 (a,b) 的过程，从而节省了运行时间. 算法细节请参阅

文献 [40]，其空间复杂度为 $O(m^2)$，计算时间比 AGM 算法快了一个常数. 例如，163 比特的椭圆曲线求阶，AGM 算法运行时间是 MSST 算法的 4.15 倍. 又由于 MSST 算法中的运算次数明显少于 SST 算法，所以可以说 MSST 算法是上述算法中最有效的特征为 2 的基域上的求阶算法. 但值得一提的是 MSST 算法也需要预计算，故在智能卡上实现时建议使用 AGM 算法.

第 5 章　椭圆曲线大数分解算法

整数分解问题实际包含了三个子问题：合性判定 (compositeness test)、素性判定 (primality test) 和大数分解 (integer factoring)，其中合性判定是判断整数 n 是否是合数；素性判定则是在几乎确定 n 是素数的情况下，证明 n 的确是素数；大数分解则是已知一个合数 n，求取其所有的素因子. 本章和下一章将分别介绍椭圆曲线在大数分解和素性判定中的应用.

本章讨论的大数分解问题限定为已知 n 是两个素数的乘积，求解素数 p, q，使得 $n = pq$. 该问题目前仍然是个公认的难题，即还没有多项式时间的大数分解算法. 椭圆曲线大数分解算法是 Lenstra[68] 于 1987 年提出的，该算法需要利用 $\mathbb{Q}$ 上的椭圆曲线 $E: Y^2 = X^3 + aX + b$ 和 E 在 $\mathbb{Q}$ 上的一个点 P. 而对于任意的椭圆曲线，求解其在 $\mathbb{Q}$ 上的点并非易事，故一般采用下述两种方法来获得满足要求的 (E, P).

(1) 在 $\mathbb{Z}$ 中随机选择 a, x, y，令 $b = y^2 - x^3 - ax$，则 $E: Y^2 = X^3 + aX + b, P = (x, y)$.

(2) 取椭圆曲线 E 为 $Y^2 = X^3 + aX - a, a \in \mathbb{N}$，则 $P = (1, 1)$ 是 E 在 $\mathbb{Q}$ 上的点，即 (E, P) 为所求.

5.1　Pollard $p-1$ 算法

在介绍椭圆曲线大数分解算法之前，首先给出一个与其有相同思想的经典的分解算法，即 Pollard $p-1$ 算法.

算法 5.1 (Pollard $p-1$ 算法)

输入　合数 n.

输出　n 的一个非平凡因子.

(1) 选择 $B \in \mathbb{N}, k \in \mathbb{N}$ 满足 $k = \text{1cm}(1, \cdots, B)$:

(2) 从集合 $\{2, \cdots, n-2\}$ 中随机选择 a;

(3) 计算 $a^k (\text{mod} n)$;

(4) 计算 $d = \gcd(a^k - 1, n) = \gcd((a^k - 1)(\text{mod} n), n)$;

(5) 如果 $d \neq 1, n$，输出 d;

(6) 返回第 (2) 步，或第 (1) 步重新选择 k.

定理 5.1.1 设合数 n 的某个素因子 p，若能整除 $p-1$ 的素因子的方幂均小于 B，即若 $q^{\alpha}|p-1, \alpha \in \mathbb{N}, q$ 是素数，必有 $q^{\alpha} < B$，则算法 可能输出 n 的某个因子，该因子可以被 p 整除.

证明 已知能整除 $p-1$ 的素因子的方幂均小于 B，则 $p-1|k$， $a^k \equiv 1(\mathrm{mod} p)$，故 $p|a^k-1, p|n$，即 $p|\gcd(a^k-1, n)$. 若 $a^k \equiv 1(\mathrm{mod} n)$，则算法失败，需要重新选择 $a \in \{2, \cdots, n-2\}$.

如果 n 的每一个素因子 p，均满足 $p-1$ 有大素因子，则算法失效. 而椭圆曲线大数分解算法不存在该问题.

5.2 模 n 约化

设 n 是奇合数， $p > 3$ 是 n 的一个未知的素因子.

定义 5.2.1 设 $m \in \mathbb{N}, x_1 = \dfrac{r_1}{s_1}, x_2 = \dfrac{r_2}{s_2}, r_1, r_2, s_1, s_2 \in \mathbb{Z}, s_1 \neq 0, s_2 \neq 0, \gcd(s_1, m) = \gcd(s_2, m) = 1$，如果 $x_1 - x_2 = \dfrac{r_3}{s_3}, r_3, s_3 \in \mathbb{Z}, s_3 \neq 0, \gcd(r_3, s_3) = 1, r_3 \equiv 0 \mod m$，则记作 $x_1 \equiv x_2 \mod m$.

上述定义的 $\equiv \mod m$ 是等价关系：反身性和对称性显然；若 $x_1 \equiv x_2 \mod m, x_2 \equiv x_3 \mod m$，即存在 $r, s, u, v \in \mathbb{Z}$，使得

$$x_1 - x_2 = \frac{r}{s},$$
$$x_2 - x_3 = \frac{u}{v},$$

其中， $\gcd(r, s) = \gcd(u, v) = 1, m|r, m|u$，则

$$x_1 - x_3 = x_1 - x_2 + x_2 - x_3 = \frac{r}{s} + \frac{u}{v} = \frac{rv + us}{sv}.$$

因为 $\gcd(m, sv) = 1, m|rv + us$，所以 $x_1 \equiv x_3 \mod m$. 从而也满足传递性，所以 $\equiv \mod m$ 是等价关系. 该定义实际上是对整数上模 m 的推广.

引理 5.2.2 对于任意有理数 $x_1 = \dfrac{r_1}{s_1}$, 若 $\gcd(s_1, m) = 1$，则存在唯一的整数 $x_2 \in \{0, \cdots, m-1\}$，使得 $x_1 \equiv x_2 (\mathrm{mod} m)$.

证明 因为 $\gcd(s_1, m) = 1$，所以存在 $k, t \in \mathbb{Z}$，使得 $ks_1 + tm = 1$，则 $r_1 = r_1 k s_1 + r_1 t m$， $\dfrac{r_1}{s_1} - r_1 k = \dfrac{r_1 t m}{s_1}$，故 $\dfrac{r_1}{s_1} \equiv r_1 k (\mathrm{mod} m)$，取 x_2 为 $r_1 k$

模 m 所得的非负整数即可.

下证唯一性. 若存在 $x_2' \in \{0,\cdots,m-1\}, x_2' \equiv x_1(\bmod m)$ ，则 $x_2' \equiv x_2(\bmod m)$ ，所以 $x_2' = x_2$. 结论证毕.

设定义在 $\mathbb{Z}$ 上的椭圆曲线 $E: Y^2 = X^3 + aX + b$ ，其在 $\mathbb{Q}$ 上的点 P ，椭圆曲线大数分解算法需要计算 $kP(\bmod n)$ ，为使计算有效, 必须要求 P 的各坐标以及所有中间点的各坐标的分母均与 n 互素.

引理 5.2.3 设椭圆曲线 $E: Y^2 = X^3 + aX + b, a, b \in \mathbb{Z}, \gcd(4a^3 + 27b^2, n) = 1$ ， P_1, P_2 是 E 在 $\mathbb{Q}$ 上的两个点, 其各坐标的分母均与 n 互素, $P_1 \neq -P_2$ ，则 $P_1 + P_2$ 的各坐标的分母与 n 互素当且仅当对所有的素数 $p|n$ ，均有

$$P_1(\bmod p) + P_2(\bmod p) \neq O(\bmod p),$$

其中, $O(\bmod p)$ 是指 $E(\bmod p)$ 上的无穷远点, $E(\bmod p)$ 是将 E 的所有系数模 p 所得的 $\mathbb{F}_p$ 上的椭圆曲线.

证明 为描述方便, 以下 $P_1 + P_2 = O(\bmod p)$ 指在 $E(\bmod p)$ 上运算. 设 $P_1 = (x_1, y_1), P_2 = (x_2, y_2)$, 则 $P_1 + P_2 = (x_3, y_3)$ ，其中

$$\lambda = \begin{cases} \dfrac{y_2 - y_1}{x_2 - x_1}, & P_1 \neq P_2 \\ \dfrac{3x_1^2 + a}{2y_1}, & P_1 = P_2 \end{cases}$$

$$x_3 = \lambda^2 - x_1 - x_2,$$

$$y_3 = \lambda(x_1 - x_3) - y_1.$$

若 $P_1, P_2, P_1 + P_2$ 的各坐标的分母均与 n 互素, 要证明对于所有的素数 $p|n$ ，在模 p 意义下 $P_1 + P_2 \neq O$. 对于给定的素数 $p|n$:

(1) 若 $x_1 \not\equiv x_2(\bmod p)$ ，显然 $P_1 + P_2 \neq O(\bmod p)$.

(2) 若 $x_1 \equiv x_2(\bmod p)$:

①如果 $P_1 = P_2$ ，则 $P_1 + P_1 = 2P_1$. 如果 $2P_1 = O(\bmod p)$ ，则 $2y_1 \equiv 0(\bmod p)$ ，因为 $2P_1$ 的分母与 n 互素， $p|n$ ，所以 $3x_1^2 + a \equiv 0(\bmod p)$ ，则 $P_1(\bmod p)$ 是 $E(\bmod p)$ 的奇异点, 而由 $\gcd(4a^3 + 27b^2, n) = 1$ 知 $E(\bmod p)$ 是椭圆曲线, 矛盾, 故 $2P_1 \neq O(\bmod p)$.

②如果 $P_1 \neq P_2$ ，则 $x_1 \equiv x_2 \mod p, x_1 \neq x_2$ ，所以存在整数 $l \geqslant 1, r \not\equiv 0 \mod p, s \not\equiv 0 \mod p$ ，使得 $x_2 = x_1 + p^l x, x = \frac{r}{s}$. 因为 $P_1 + P_2$ 的坐标的分母

与 n 互素，所以 $y_2=y_1+p^l y, y\in\mathbb{Q}, y$ 的分母不能被 p 整除. 另一方面，

$$\begin{aligned}
y_2^2&=(x_1+p^l x)^3+a(x_1+p^l x)+b\\
&=x_1^3+3p^l x x_1^2+3(p^l x)^2 x_1+(p^l x)^3+ax_1+ap^l x+b\\
&=x_1^3+ax_1+b+p^l x(3x_1^2+3p^l x x_1+a+p^{2l}x^2)\\
&=y_1^2+p^l x(3x_1^2+a) \mod p^{l+1}.
\end{aligned}$$

因为 $x_1\equiv x_2 \mod p, y_2\equiv y_1 \mod p$, 所以 $P_1 \mod p=P_2 \mod p, P_1+P_2=2P_1 \mod p$. 那么 $P_1+P_2=O \mod p$ 当且仅当 $2P_1=O \mod p$ ，当且仅当 $y_1\equiv -y_2 \mod p$. 如果 $y_1\equiv -y_2 \mod p$ ，则 $y_1\equiv y_2\equiv 0 \mod p, x_1^3+ax_1+b=0 \mod p$. 因为 $p^l|y_1-y_2$ ，所以 $y_2^2-y_1^2\equiv 0 \mod p^{l+1}$ ，但由上式知 $y_2^2-y_1^2\equiv p^l x(3x_1^2+a) \mod p^{l+1}$ ，故 $3x_1^2+a\equiv 0 \mod p$ ，即 $P_1 \mod p$ 是 $E \mod p$ 的奇异点，矛盾，故 $P_1+P_2\neq O \mod p$.

设对于所有的素数 $p|n$ ， $P_1+P_2\neq O \mod p$ ，要证明 P_1+P_2 的坐标的分母与 n 互素. 对于给定的素数 $p|n$:

(1) 若 $x_1\not\equiv x_2 \mod p$, 则由加法公式知 P_1+P_2 的坐标的分母与 p 互素;

(2) 若 $x_1\equiv x_2 \mod p$, 则 $y_1\equiv \pm y_2 \mod p$, 因为 $P_1+P_2\neq O \mod p$, 所以 $y_2\equiv y_1\not\equiv 0 \mod p$.

①如果 $P_1=P_2$ ，由加法公式以及 $y_1\not\equiv 0 \mod p$ ，知 $P_1+P_2=2P_1$ 的坐标的分母与 p 互素;

②如果 $P_2\neq P_1$ ，则存在 $l\geqslant 1, x\in\mathbb{Q}$ ，使得 $x_2=x_1+p^l x$ ，同上计算可得

$$\frac{y_2^2-y_1^2}{x_2-x_1}\equiv 3x_1^2+a \mod p.$$

因为 $y_2+y_1\equiv 2y_1 \mod p$ ，所以 p 不整除 y_2+y_1 ，即

$$\frac{y_2-y_1}{x_2-x_1}=\frac{y_2^2-y_1^2}{(y_2+y_1)(x_2-x_1)}$$

的分母与 p 互素，由加法公式知 P_1+P_2 的坐标的分母与 p 互素. 结论证毕.

5.3 Lenstra 算法

对于给定的奇合数 n ，选择 $\mathbb{Q}$ 上的椭圆曲线 $E: Y^2 = X^3 + aX + b$ ，及其 E 在 $\mathbb{Q}$ 上的一点 $P = (x, y)$. 取定 $B, C \in \mathbb{N}$ ，令

$$k = \prod_{p_i \leqslant B} p_i^{\alpha_i},$$

其中， $\alpha_i = [\log C / \log p_i]$ ，计算 $kP \mod n$ ，设 $P_1 + P_2 \mod n$ 是某个中间过程， $P_1 = (x_1, y_1), P_2 = (x_2, y_2), P_1 \neq P_2$ ，如果 $\gcd(x_2 - x_1, n) \neq 1$ ，则计算无法继续；同理，若 $P_1 = P_2$ ， $\gcd(2y_1, n) \neq 1$ ，则计算也无法继续. 但在这两种情况下，可以求得 n 的因子. 由引理 5.2.2 知上述情况发生，当且仅当存在素数 $p|n, k_1 \leqslant k$ ，使得 $k_1 P = O \mod p$ ，这时对和点的坐标的分母求逆便转为求分母与 n 的公因子. 如果该公因子等于 n ，则说明对于任意的 $p|n$ ，均有 $k_1 P = O \mathrm{mod} p$ ，该事件是几乎不可能发生的，故公因子是 n 的非平凡因子.

上述介绍的椭圆曲线大数分解算法： Lenstra 算法的思想和 Pollard $p-1$ 算法是一致的，但 Pollard $p-1$ 算法考虑 n 的素因子 p 所决定的乘法群 $\mathbb{F}_p^\times$ ，而 Lenstra 算法考虑的是椭圆曲线群 E 和其上的点 P ， E, P 的选择范围较大，从而 Lenstra 算法更加灵活.

算法 5.2 (Lenstra 算法)

输入 奇合数 n.

输出 n 的非平凡因子.

(1) 选择 $(E, P), E: Y^2 = X^3 + aX + b, a, b \in \mathbb{Z}, P$ 是 E 在 $\mathbb{Z}$ 上的点；

(2) 计算 $d = \gcd(4a^3 + 27b^2, n)$ ，若 $d \neq 1, n$ ，则输出 d ；若 $d = n$ ，则返回第 (1) 步；

(3) 选择 $B, C \in \mathbb{N}$ ；

(4) 计算 $k = \prod\limits_{\text{素数} l \leqslant B} l^{\alpha_l}, \alpha_l = [\log C / \log l]$ ；

(5) 计算 $kP \mod n$ ，若计算无法继续，即某个中间结果所得的有理数的分母 s 无法在模 n 下求逆，则计算 $d = \gcd(s, n)$ ，如果 $d \neq n$ ，则输出 d ；否则，返回第 (1) 步.

5.4 时间复杂度

本节将分析 Lenstra 算法的时间复杂度，首先给出一些假设：奇合数 n 不是素数的方幂；随机选择 $a, x, y \in \mathbb{Z}$，令

$$E: Y^2 = X^3 + aX + (y^2 - x^3 - ax),$$
$$P = (x, y);$$

kP 是按 k 的分解计算的，即若

$$k = \prod_{i=1}^{m} p_i^{\alpha_i}, \quad \alpha_i \in \mathbb{N},$$

其中 p_i 是互不相同的素数，则

$$kP = (p_m^{\alpha_m} \cdots (p_2^{\alpha_2}(p_1^{\alpha_1} P)) \cdots),$$

该方法实际上计算了所有的 $dP, d = \prod_{i=1}^{l} p_i^{\alpha'_i}, 0 < \alpha'_l \leqslant \alpha_l$，对于 $0 < i < l$，有 $\alpha'_i = \alpha_i$，这使得若 P 的阶是 k 的小因子的话，Lenstra 算法的本次运行可以快速结束.

引理 5.4.1 设素数 $p \neq 2, 3$，则定义在 $\mathbb{F}_p$ 上的形如 $Y^2 = X^3 + aX + b$ 的椭圆曲线的个数为 $p^2 - p$.

证明 $Y^2 = X^3 + aX + b$ 是椭圆曲线，意味着 $\gcd(4a^3 + 27b^2, p) = 1$. 显然 $a = 0, b = 0$ 是不可取的；设 3 是 $\mathbb{F}_p$ 中的二次剩余，若 a 是二次剩余，则存在两个 $b \in \mathbb{F}_p$，使得 $4a^3 + 27b^2 \equiv 0 \mod p$，若 a 是二次非剩余，则 $4a^3 + 27Y^2 \equiv 0 \mod p$ 在 $\mathbb{F}_p$ 中无解，所以一共有 p 对 $(a, b) \in \mathbb{F}_p^2$，使得 $4a^3 + 27b^2 \equiv 0 \mod p$；设 3 是 $\mathbb{F}_p$ 中的二次非剩余，若 a 是二次非剩余，则存在两个 $b \in \mathbb{F}_p$，使得 $4a^3 + 27b^2 \equiv 0 \mod p$，若 a 是二次剩余，则 $4a^3 + 27Y^2 \equiv 0 \mod p$ 在 $\mathbb{F}_p$ 中无解，所以一共有 p 对 $(a, b) \in \mathbb{F}_p^2$，使得 $4a^3 + 27b^2 \equiv 0 \mod p$；综上所述，在 p^2 对 $(a, b) \in \mathbb{F}_p^2$ 中有 p 对，其所确定的不是椭圆曲线，所以形如 $Y^2 = X^3 + aX + b$ 的椭圆曲线有 $p^2 - p$ 条.

当 $p \neq 2, 3$ 时，$\mathbb{F}_p$ 上的椭圆曲线均同构于某个形如 $Y^2 = X^3 + aX + b$ 的椭圆曲线，由 Hasse 定理知 $\mathbb{F}_p$ 上椭圆曲线的阶有 $4\sqrt{p} + 1$ 个可能取值，再由上

述引理知有 p^2-p 条椭圆曲线，所以可能有 $\dfrac{p^2-p}{4\sqrt{p}+1}\approx p\sqrt{p}$ 条椭圆曲线拥有相同的阶.

定理 5.4.2 (Deuring) 设素数 $p\neq 2,3$，则存在整数 $c>0$，使得对于任意的 $t\in\mathbb{Z},|t|\leqslant 2\sqrt{p}$，一共有 $\dfrac{cp\sqrt{p}}{\ln p}$ 条定义在 $\mathbb{F}_p$ 上的椭圆曲线的阶为 $p+1-t$.

定理 5.4.3 (Lenstra) 设素数 $p\neq 2,3$，则存在整数 $c>0$，使得对于任意的 $l\in\mathbb{N}$，至少有 cp^2 条定义在 $\mathbb{F}_p$ 上的椭圆曲线的阶模 l 不等于 0.

定义 5.4.4 设 $y\in\mathbb{R}^+$，自然数 n 称为 y 光滑的，如果 n 的所有素因子均不大于 y.$\Psi(x,y)$ 表示不大于自然数 x 的 y 光滑自然数的个数，即

$$\Psi(x,y)=|\{n\in\mathbb{N}:n\leqslant x,n\text{是}y\text{光滑的}\}|.$$

对于 $n\in\mathbb{N}$，定义

$$L(n)=\mathrm{e}^{\sqrt{\ln n\ln\ln n}},$$

$$L_n(\beta)=L(n)^\beta=\mathrm{e}^{\beta\sqrt{\ln n\ln\ln n}}.$$

定理 5.4.4 (Canfield,Erdös,Pomerance) 设 $x,y\in\mathbb{N}$，令 $u=\dfrac{\ln x}{\ln y}$，如果存在 $\varepsilon>0$，使得 $\ln^\varepsilon x<u<\ln^{1-\varepsilon}x$，则当 x 趋于 ∞ 时，$\Psi(x,y)=xu^{-u(1+o(1))}$ 为均匀分布，其中 $o(1)$ 表示 n 趋于 ∞ 时，其值趋于 0 的函数.

推论 5.4.5 对于 $x,a\in\mathbb{N}$，有

$$\Psi(x,L(x)^a)=xL(x)^{-\frac{1}{2a}+o(1)}.$$

证明 令 $u=\dfrac{\ln x}{\ln(L(x)^a)}$，因为 $L(x)^a=\mathrm{e}^{a\sqrt{\ln x\ln\ln x}}$，即 $\ln(L(x)^a)=a(\ln x\ln\ln x)^{\frac{1}{2}}$，所以

$$u=\frac{\ln^{\frac{1}{2}}x}{a\ln^{\frac{1}{2}}\ln x}=\mathrm{e}^{\ln\ln^{\frac{1}{2}}x-\ln a-\ln\ln^{\frac{1}{2}}\ln x}.$$

令 $\varepsilon=\frac{1}{4}$，则 $\ln^\varepsilon x<u<\ln^{1-\varepsilon}x$，满足定理 5.4.4 的要求，故当 x 趋于 ∞ 时，$\Psi(x,L(x)^a)=xu^{-u(1+o(1))}$，而

$$u^{-u(1+o(1))}=\mathrm{e}^{\left(\frac{1}{2}\ln\ln\ln x+\ln a-\frac{1}{2}\ln\ln x\right)\left(\frac{\ln^{\frac{1}{2}}x}{a\ln^{\frac{1}{2}}\ln x}(1+o(1)\right)}$$

$$= \mathrm{e}^{\left(\frac{\ln\ln\ln x}{\ln\ln x}\frac{1}{2a}\sqrt{\ln x\ln\ln x}+\frac{2\ln a}{\ln\ln x}\frac{\sqrt{\ln x\ln\ln x}}{2a}-\frac{1}{2a}\sqrt{\ln x\ln\ln x}\right)(1+o(1))}$$
$$= L(x)^{-\frac{1}{2a}(1+o(1))}$$

所以 $\Psi(x, L(x)^a) = xL(x)^{-\frac{1}{2a}+o(1)}$.

令 m_p 为 P 在 $E \mod p$ 中的阶, 设 n 是两个奇素数 p, q 的乘积, 且 Lenstra 算法选择的 (E, P, B, C) 满足以下要求:

(1) $m_p = \prod\limits_{i=1}^{m} {p_i}^{\alpha_i}, p_i \leqslant B, p_i^{\alpha_i} \leqslant C$;

(2) $m_p P \neq O \mod q$(否则, 所求得的公因子为 n).

在上述要求下, Lenstra 算法将输出 n 的某个非平凡因子.

定理 5.4.6 设 $n \in \mathbb{N}$, 若存在奇素数 $p \neq q, p|n, q|n$, 且 Lenstra 算法选择的 (E, P) 满足:

(1) $p \leqslant B_2$, $B_2 + 2\sqrt{B_2} + 1 \leqslant C$;

(2) $m_1 = |E(\mathbb{F}_p)|$ 的素因子均小于 B;

(3) $m_2 = |E(\mathbb{F}_q)|$ 不能被 $P \mod p$ 的阶的最大素因子整除.

则 Lenstra 算法输出 n 的非平凡因子.

证明 因为 $p \leqslant B_2$, 所以

$$\begin{aligned}|E(\mathbb{F}_p)| &\leqslant |p + 2\sqrt{p} + 1| \\ &\leqslant B_2 + 2\sqrt{B_2} + 1 \\ &\leqslant C.\end{aligned}$$

而 $m_p||E(\mathbb{F}_p)|$, 故 $m_p = \prod\limits_{i=1}^{t} p_i^{\alpha_i}, p_1 < p_2 < \cdots < p_t \leqslant B, p_i^{\alpha_i} \leqslant m_p \leqslant C, i = 1, \cdots, t$. 若 $p_t \nmid m_2$, 则 $p_t \nmid m_q$, 即 $m_p \nmid m_q$, 若 $m_q < m_p, m_q|m_p$, 则 $m_q = \prod\limits_{i=1}^{t-1} p_i^{\alpha'_i}, \alpha'_i \leqslant \alpha_i, i = 1, \cdots, t-1$, 且 $m_q P = O \mod q$, 所以 Lenstra 算法在计算 $k'P, k' = p_{t-1}^{\alpha'_{t-1}} \prod\limits_{i=1}^{t-2} p_i^{\alpha_i}$ 时, 已经求得 q 并输出; 若 $m_q \nmid m_p$, 则 $m_p P \neq O \mod q$, Lenstra 算法在计算 $m_p P$ 时, 可以求得 p 并输出.

设 $E: Y^2 = X^3 + aX + b$, 素数 $p|n, q|n$, 令 $\tilde{n} = pq, \tilde{n}|n$, 则对于任意的 $\alpha \in \mathbb{F}_p, \beta \in \mathbb{F}_q, \gamma \in \mathbb{Z}_{\tilde{n}}, \gamma \equiv \alpha \mod p, \gamma \equiv \beta \mod q$, 有

$$\begin{aligned}\text{Prob}(a \mod p = \alpha | a \mod q = \beta) &= \frac{\text{Prob}(a \mod p = \alpha, a \mod q = \beta)}{\text{Prob}(a \mod q = \beta)} \\ &= \frac{\text{Prob}(a \mod \tilde{n} = \gamma)}{\text{Prob}(a \mod q = \beta)} \\ &= \frac{\frac{1}{pq}}{\frac{1}{q}} \\ &= \frac{1}{p} \\ &= \text{Prob}(a \mod p = \alpha).\end{aligned}$$

所以 $a \mod p$ 与 $a \mod q$ 无关，故 $E \mod p$ 和 $E \mod q$ 也无关.

引理 5.4.7 设 $a, x, y \in_R \mathbb{Z}$，若 n 的所有素因子均大于 B，则 $\gcd(4a^3 + 27b^2, n) \neq 1$ 的概率不大于 $\frac{2}{\sqrt{B}} \log_B n$.

证明 对于素数 p，由引理 5.4.1 知 $\mathbb{F}_p$ 上形如 $Y^2 = X^3 + aX + b$ 的椭圆曲线有 $p^2 - p$ 条，而每条椭圆曲线至少有 $p - 2\sqrt{p}$ 个有限点，则 Lenstra 算法中可选的 (E, P) 的个数至少为

$$(p^2 - p)(p - 2\sqrt{p}) \geqslant p^3 - 2p^{\frac{5}{2}}.$$

所以，对于随机选择的 $a, x, y \in \mathbb{Z}$，恰好决定了一对可用的 $(E \mod p, P \mod p)$ 的概率至少为 $1 - \frac{2}{\sqrt{p}}$，则

$$\text{Prob}_{(a,x,y) \in_R \mathbb{Z}^3}(4a^3 + 27b^2 \equiv 0 \mod p) \leqslant \frac{2}{\sqrt{p}}.$$

若 n 的所有素因子均大于 B，则 n 的素因子个数小于 $\log_B n$，故

$$\text{Prob}_{(a,x,y) \in_R \mathbb{Z}^3}(\text{存在素数} p | n, 4a^3 + 27b^2 \equiv 0 \mod p) \leqslant \sum_{p|n} \frac{2}{\sqrt{p}} \leqslant \frac{2 \log_B n}{\sqrt{B}}.$$

定理 5.4.8 设 n 是奇合数，素数 $p|n, p \leqslant B_2$，u 表示 $[p - 2\sqrt{p} + 1, p + 2\sqrt{p} + 1]$ 间 B 光滑自然数存在的概率，则存在整数 $c_0 > 0$，使得对于 $(a, x, y) \in_R \mathbb{Z}^3$，Lenstra 算法成功的概率大于 $\frac{c_0 u}{\ln p}$.

证明 设素数 $q|n, q \neq p$，要计算对于随机的 $(a,x,y) \in \mathbb{Z}^3$，其所确定的 (E,P) 满足下述条件的概率:

(1) $|E(\mathbb{F}_p)|$ 是 B 光滑的;

(2) $|E(\mathbb{F}_q)|$ 不能被 $P \mod p$ 的阶 m_p 的最大素因子整除.

因为 $[p-2\sqrt{p}+1, p+2\sqrt{p}+1]$ 间的 B 光滑自然数有 $4u\sqrt{p}$ 个, 由定理 5.4.2 知存在 $c_1 > 0$，使得对于 $t \in [p-2\sqrt{p}+1, p+2\sqrt{p}+1]$，至少有 $\dfrac{c_1 p\sqrt{p}}{\ln p}$ 条椭圆曲线的阶为 t，而每条椭圆曲线上有限点的个数至少为 $p-2\sqrt{p}$，所以

$$\begin{aligned}\mathrm{Prob}_{(a,x,y)\in_R\mathbb{Z}^3}((E,P)|\ |E(\mathbb{F}_p)|\text{是}B-\text{光滑的}) &\geqslant \frac{(4u\sqrt{p})(c_1p\sqrt{p})(p-2\sqrt{p})}{p^3\ln p}\\ &= \frac{4uc_1p^2(p-2\sqrt{p})}{p^3\ln p} \geqslant \frac{c_2u}{\ln p},\end{aligned}$$

其中, $0 < c_2 \leqslant \dfrac{4c_1(p-2\sqrt{p})}{p}$.

设 p' 是 m_p 的最大素因子, 注意到 $P(\mathrm{mod} p)$ 和 $P(\mathrm{mod} q)$ 无关, 即在 m_p 给定的条件下, $E(\mathrm{mod} q), P(\mathrm{mod} q)$ 均随机. 由定理 5.4.3 知存在 $c_3 > 0$，使得

$$\begin{aligned}|\{(E,P): p' \nmid |E(\mathbb{F}_q)|\}| &\geqslant |\{E: p' \nmid |E(\mathbb{F}_q)|\}| \cdot (|E(\mathbb{F}_q)|-1)\\ &\geqslant c_3q^2(q-2\sqrt{q}), \qquad c_3 > 0\\ &\geqslant c_4q^3, \qquad 0 < c_4 < c_3\left(1-\frac{2}{\sqrt{q}}\right)\end{aligned}$$

已证明 $E(\mathrm{mod} p)$ 和 $E(\mathrm{mod} q)$ 无关, 所以对于随机的 $(a,x,y) \in \mathbb{Z}^3$，其所确定的 (E,P) 满足上述两个条件的概率大于 $\dfrac{c_0u}{\ln p}, c_0 = c_2c_4$.

对于 $[p-2\sqrt{p}+1, p+2\sqrt{p}+1]$ 间 B 光滑自然数存在的概率给出如下假设.

假设 令 $B = L_p(\beta)$，则 $[p-2\sqrt{p}+1, p+2\sqrt{p}+1]$ 间 B 光滑自然数存在的概率为 $L_p\left(\dfrac{-1}{2\beta}\right)$.

以下的讨论均基于该假设.

推论 5.4.9 设奇合数 n 有素因子 $p \leqslant B_2$，令 $B = L_{B_2}(\beta)$，则 Lenstra 算法成功输出所需的运行次数的期望值不大于

$$\frac{1}{c_0}\ln B_2 L_{B_2}\left(\frac{1}{2\beta}\right).$$

证明 由定理 5.4.8 和假设知，Lenstra 算法运行一次成功的概率大于$\dfrac{c_0L_p\left(\frac{-1}{2\beta}\right)}{\ln p}$，而

$$\frac{c_0L_p\left(\frac{-1}{2\beta}\right)}{\ln p}\geqslant\frac{c_0L_{B_2}\left(\frac{-1}{2\beta}\right)}{\ln B_2},$$

所以 Lenstra 算法成功输出所需的运行次数的期望值小于 $\dfrac{1}{c_0}\ln B_2L_{B_2}\left(\dfrac{1}{2\beta}\right)$.

推论 5.4.10 Lenstra 算法的运行时间的期望值为 $O\left(L_{B_2}\left(\dfrac{1}{2\beta}\right)L_{B_2}(\beta+o(1))\ln^2 n\right)$ 次比特运算.

证明 Lenstra 算法的运行时间由算法的第 (5) 步决定，而该步运行一次至多需要进行 $\sum\limits_{i=1}^{m}\alpha_i\ln p_i$ 次椭圆曲线的点加，其中 $m\leqslant B,\alpha_i\leqslant\ln B_2,p_i\leqslant B,i=1,\cdots,m$，故

$$\sum_{i=1}^{m}\alpha_i\ln p_i\leqslant B\ln B\ln B_2=L_{B_2}(\beta)\ln L_{B_2}(\beta)\ln B_2=L_{B_2}(\beta+o(1)).$$

每个椭圆曲线点加需要常数次模 n 的乘法，而模 n 的乘法需要 $O(\ln^2 n)$ 次比特运算，所以 Lenstra 算法运行时间的期望值等于运行次数的期望值与每一次运行所需时间的乘积，由推论 5.4.9 知，其值为

$$O\left(\ln B_2L_{B_2}\left(\frac{1}{2\beta}\right)L_{B_2}(\beta+o(1))\ln^2 n\right)=O\left(L_{B_2}\left(\frac{1}{2\beta}\right)L_{B_2}(\beta+o(1))\ln^2 n\right).$$

定理 5.4.11 设奇合数 n 至少有两个不同的素因子，则 Lenstra 算法的期望运行时间至多为 $\mathrm{e}^{(1+o(1))\sqrt{\ln n\ln\ln n}}$.

证明 n 一定有一个小于 $\sqrt{n}$ 的素因子，所以令 $B_2=\sqrt{n}$，则由推论 5.4.10 知，Lenstra 算法的运行时间为

$$L_{\sqrt{n}}\left(\frac{1}{2\beta}\right)L_{\sqrt{n}}(\beta+o(1))\ln^2 n=L_{\sqrt{n}}\left(\frac{1}{2\beta}\right)L_{\sqrt{n}}(\beta+o(1)).$$

设 $f(x)=\dfrac{1}{2x}+x,x\in\mathbb{R}$，则 $f'(x)=\dfrac{4x^2-2}{4x^2},f''(x)=\dfrac{1}{x^3}$，故 $f'\left(\dfrac{1}{\sqrt{2}}\right)=0,f''\left(\frac{1}{\sqrt{2}}\right)>0$，即 $x=\dfrac{1}{\sqrt{2}}$ 时，$f(x)$ 有最小值 $\sqrt{2}$，令 $\beta=\dfrac{1}{\sqrt{2}}$，将其代入上式，即得结论.

从以上分析知，对于至少有两个不同的素因子的奇合数 n ， Lenstra 算法中的 $B = L_{\sqrt{n}}\left(\frac{1}{\sqrt{2}}\right), C = \sqrt{n} + 2\sqrt[4]{n} + 1$ 时，算法的期望运行时间至多为 $\mathrm{e}^{(1+o(1))\sqrt{\ln n \ln\ln n}}$.

对于形如 pq 的随机整数而言， p, q 是相同尺寸的素数的概率是非常小的，所以椭圆曲线大数分解算法要优于二次筛法和数域筛法. 但是，基于大数分解问题的公钥密码体制均使用的是相同尺寸的素数 p, q 所得到的合数 $n = pq$ ，故而椭圆曲线大数分解算法在密码中的使用是比较受限的.

第 6 章　椭圆曲线素性判定算法

椭圆曲线素性判定算法是 1986 年由 Goldwasser 和 Kilian 提出的，随后 Atkin 将其改进成为一个实用算法，其期望运行时间为 $O(\ln^6 n)$ ，其中 n 为需判定的数. 本章首先介绍 Atkin 算法所需的相关知识，即带复乘的椭圆曲线，随后描述 Goldwasser-Kilian 算法，最后给出 Atkin 算法.

6.1　带复乘的椭圆曲线

数域 K 是 $\mathbb{Q}$ 上的 n 次代数扩张，若 $\alpha \in K$ ，且存在首一的整系数多项式 $f \in \mathbb{Z}[X], f(\alpha) = 0$ ，则称 α 为 K 中的代数整数. O_K 表示 K 中所有代数整数构成的环，则 O_K 的任意非零理想均是秩为 n 的自由 $\mathbb{Z}$ 模， O_K 的一组 $\mathbb{Z}$ 基称为 K 的整基. 若 I 是 O_K 模，且存在 $\alpha \in O_K$ 使得 αI 是 O_K 的理想，则称 I 为 O_K 的分式理想. 设 $\sigma_i, i = 1, \cdots, n$ 是 K 到 $\mathbb{C}$ 的 n 个嵌入， $\alpha_j, j = 1, \cdots, n$ 是 K 的 n 个元素，则有

$$\det(\sigma_i(\alpha_j))^2 = \det(\mathrm{Tr}_{K/\mathbb{Q}}(\alpha_i\alpha_j)).$$

该值称为 α_i 的判别式，记作 $d(\alpha_1, \cdots, \alpha_n)$.$d(\alpha_1, \cdots, \alpha_n) = 0$ 当且仅当 α_j 是 $\mathbb{Q}$ 线性相关的. 已证明，若 α_j 均为代数整数，则 $d(\alpha_1, \cdots, \alpha_n) \equiv 0, 1 \mod 4$.$K$ 的整基的判别式称为 K 的判别式，记作 $d(K)$.

K 的 order 是 K 的子环，且是有限生成的 $\mathbb{Z}$ 模，其秩至多为 n.O_K 是 K 的极大 order ，以下若没有特殊说明，则 order 均指极大 order. 设 p 是素数，则存在 O_K 的素理想 $\mathbf{p}_i, i = 1, \cdots, g$ ，使得

$$pO_K = \prod_{i=1}^{g} \mathbf{p}_i^{e_i}.$$

(1) 若 $g = 1, e_1 = 1$ ，则称 p 是惰性的 (inert)；

(2) 若 $g = n, e_i = 1$ ，则称 p 是完全分裂的 (split completely).

(3) 如果存在某个 $e_i \geqslant 2$ ，则称 p 是分歧的 (ramified)；

(4) 否则，称为非分歧的 (unramified).

已有结论，在判别式为 D 的二次数域 K 中，对于素数 p:

(1) 若 $\left(\dfrac{D}{p}\right)=-1$ ，则 p 是惰性的;

(2) 若 $\left(\dfrac{D}{p}\right)=0$ ，则 p 是分歧的;

(3) 若 $\left(\dfrac{D}{p}\right)=1$ ，则 p 完全分裂.

K 的两个分式理想 I,J 称为等价的，若存在 $\alpha\in K^{\times}$ ，使得 $J=\alpha I$. 所有的分式理想等价类组成的集合是一个有限 Abel 群，称为 O_K 或 K 的类群 (class group)，记作 $Cl(K)$，其阶称为类数 (class number)，记作 $h(K)$. 若 $x\in K$ ，x,x^{-1} 均为代数整数，则称 x 为 K 的单位 (unit)， K 的所有单位构成一个乘法群，记作 $U(K)$，其中单位根的全体组成的群记作 $\mu(K)$， $\mu(K)$ 是有限循环群.

设 $K=\mathbb{Q}(\sqrt{d})$ 是二次数域，$d\neq 1$ 且不是平方数，$1,\omega$ 是一组整基，$d(K)$ 是 K 的判别式，

(1) 若 $d\equiv 1 \mod 4$ ，则 $\omega=\dfrac{1+\sqrt{d}}{2}, d(K)=d$;

(2) 若 $d\equiv 2,3 \mod 4$ ，则 $\omega=\sqrt{d}, d(K)=4d$.

若整数 D 是二次数域 K 的判别式，称 D 为基本判别式，则 $K=\mathbb{Q}(\sqrt{D})$ ，K 的整基为

$$1,\omega=\frac{D+\sqrt{D}}{2},$$

$O_K=\mathbb{Z}[\omega]$ ， σ 表示 K 的 $\mathbb{Q}$ 线性映射，且 $\sigma(\sqrt{D})=-\sqrt{D}$ ，对于 $\alpha\in K$. 设素数 $p\neq 2$ ，

(1) 若 $\left(\dfrac{D}{p}\right)=0$ ，则 $pO_K=\mathbf{p}^2,\mathbf{p}=pO_K+\omega O_K$;

(2) 若 $\left(\dfrac{D}{p}\right)=-1$ ，则 $\mathbf{p}=pO_K$ 是素理想;

(3) 若 $\left(\dfrac{D}{p}\right)=1$ ，则 $pO_K=\mathbf{p}_1\mathbf{p}_2$, 其中

$$\begin{aligned}
\mathbf{p}_1&=pO_K+\left(\omega-\frac{D+b}{2}\right)O_K,\\
\mathbf{p}_2&=pO_K+\left(\omega-\frac{D-b}{2}\right)O_K,\\
b^2&\equiv D \mod 4p.
\end{aligned}$$

若 $D<0, D\equiv 0,1 \mod 4$ ，则 $\mu(K)$ 的阶 $\omega(D)$ 满足

$$\omega(D)=\begin{cases}2, & D<-4\\ 4, & D=-4\\ 6, & D=-3\end{cases}$$

命题 6.1.1 设 $K=\mathbb{Q}(\sqrt{D}), p$ 是素数，则 $p=N_K(X)$ 在 O_K 中有解，当且仅当 p 完全分裂，即存在 $a,b\in\mathbb{Z}$，使得 $4p=a^2-Db^2$.

设 $\omega_1,\omega_2\in\mathbb{C}$，则由 ω_1,ω_2 生成的格为 $L=\{m\omega_1+n\omega_2|m,n\in\mathbb{Z}\}$. 定义

$$\mathcal{P}(Z)=\frac{1}{Z^2}+\sum_{\omega\in L\setminus\{0\}}\left(\frac{1}{(Z+\omega)^2}-\frac{1}{\omega^2}\right).$$

$$g_2=60\sum_{\omega\in L\setminus\{0\}}\frac{1}{\omega^4}$$

$$g_3=140\sum_{\omega\in L\setminus\{0\}}\frac{1}{\omega^6}$$

则 $\mathcal{P}'^2=4\mathcal{P}^3-g_2\mathcal{P}-g_3$，且映射

$$\mathbb{C}/L\to\{(x,y,t)\in\mathbb{C}^3: y^2t=4x^3-g_2xt^2-g_3t^3\},$$

$$z\mapsto\begin{cases}(\mathcal{P}(z),\mathcal{P}'(z),1), & z\neq 0\\ (0,1,0), & z=0\end{cases}$$

是同构. 因为复环面 (torus)$\mathbb{C}/L$ 非奇异，所以代数曲线 $Y^2T=4X^3-g_2XT^2-g_3T^3$ 是非奇异的，即判别式

$$\Delta=16(g_2^3-27g_3^2)$$

不等于 0，即为椭圆曲线. 以下用 $\mathbb{C}/L$ 表示与其同构的椭圆曲线

$$Y^2T=4X^3-g_2XT^2-g_3T^3.$$

于是有下述定理.

定理 6.1.2 $\mathbb{C}$ 上的椭圆曲线均为 $\mathbb{C}/L, L$ 是格. 即，若 $g_2,g_3\in\mathbb{C}, g_2^3-27g_3^2\neq 0$，则存在 $\omega_1,\omega_2\in\mathbb{C},\omega_2/\omega_1$ 的虚部大于 0，使得

$$g_2=60\sum_{(m,n)\neq(0,0)}(m\omega_1+n\omega_2)^{-4},$$

$$g_3=140\sum_{(m,n)\neq(0,0)}(m\omega_1+n\omega_2)^{-6}.$$

命题 6.1.3 设 $E=\mathbb{C}/L, E'=\mathbb{C}/L'$ 是定义在 $\mathbb{C}$ 上的两条椭圆曲线，则：

(1) E 同构于 E' 当且仅当存在非零复数 α，使得 $L'=\alpha L$.

(2) E 到 E' 的同种构成的集合和满足 $\alpha L\subset L'$ 的复数 α 构成的集合间存在一一对应. 特别地，E 的自同态环同构于由满足 $\alpha L\subset L$ 的复数 α 构成的集合.

设定义在 $\mathbb{C}$ 上的椭圆曲线

$$E: Y^2=4X^3-g_2X-g_3,$$
$$E': Y^2=4X^3-g_2'X-g_3'$$

同构，由命题 6.1.3 知存在非零复数 α，使得

$$g_2'=\alpha^{-4}g_2,$$
$$g_3'=\alpha^{-6}g_3.$$

因为 E 非奇异，所以 $g_2^3-27g_3^2\neq 0$，则定义

$$j(E)=1728g_2^3/(g_2^3-27g_3^2),$$

显然，$j(E)$ 即为椭圆曲线 E 的 j 不变量，且同构的椭圆曲线 E,E' 有 $j(E)=j(E')$.

命题 6.1.4 定义在 $\mathbb{C}$ 上的椭圆曲线 E,E'，E 同构于 E' 当且仅当 $j(E)=j(E')$.

如果已知 E 的 j 不变量 $j(E)$，则可以构造 E 如下：

(1) 若 $j(E)=0$，则 $E: Y^2=X^3-1$.

(2) 若 $j(E)=1728$，则 $E: Y^2=X^3-X$.

(3) 否则 $E: Y^2=X^3-3cX+2c$，其中

$$c=\frac{j(E)}{j(E)-1728}.$$

设定义在 $\mathbb{C}$ 上的椭圆曲线 $E=\mathbb{C}/L$，格 L 可由两个 $\mathbb{R}$ 线性无关的复数 ω_1,ω_2 生成，适当排序后，$\tau=\dfrac{\omega_2}{\omega_1}$ 的虚部大于 0. 因为 L 乘以非零复数所得的 L'，对应的椭圆曲线 $E'=\mathbb{C}/L'$ 同构于 E，所以 $j(E)=j(E_\tau), E_\tau=\mathbb{C}/L_\tau, L_\tau$ 是由 $1,\tau$ 生成的格，还可以简记为 $j(\tau)=j(E_\tau)$. 故可以定义如下映射：

$$j:\mathcal{H}=\{\tau\in\mathbb{C},\tau\text{的虚部大于}0\}\to\mathbb{C},$$
$$\tau\mapsto j(\tau).$$

若整数 a,b,c,d 满足 $ad-bc=1$ ，则由 $a\tau+b, c\tau+d$ 生成的格等于 L_τ. 故有如下定理.

定理 6.1.5　若 $\mathbb{Z}$ 上的矩阵 $\begin{pmatrix} a & b \\ c & d \end{pmatrix}$ 可逆，则 $j\left(\dfrac{a\tau+b}{c\tau+d}\right)=j(\tau)$.

定理 6.1.6　存在正整数 $c_n, n\geqslant 1$ ，使得对于所有虚部大于 0 的复数 τ 有

$$j(\tau)=\frac{1}{q}+744+\sum_{n\geqslant 1} c_n q^n.$$

其中 $q=\mathrm{e}^{2i\pi\tau}$.

命题 6.1.7　设 E 是定义在特征为 0 的域上带复乘的椭圆曲线，则 E 的自同态环 $\mathrm{End}(E)$ 是虚二次域的 order ，即存在虚部大于 0 的复数 τ ，且 τ 是二次代数整数，使得 $\mathrm{End}(E)$ 同构于 $\mathbb{Z}+\mathbb{Z}\tau$ ， τ 是二次代数整数是指 $\tau^2-s\tau+n=0, s,n\in\mathbb{Z}, s^2-4n<0$.

证明　对于 $\mathbb{C}$ 上的椭圆曲线给出证明. 设 $E=\mathbb{C}/L$ ，则 $\mathrm{End}(E)$ 同构于集合 $\{\alpha\in\mathbb{C}|\alpha L\subset L\}$. 不妨假设 L 由 $1,\tau$ 生成，其中 $\tau\in\mathcal{H}$. 若复数 $\alpha L\subset L$ ，则存在整数 a,b,c,d 使得 $\alpha=a+b\tau, \alpha\tau=c+d\tau$ ，令 $e=a+d, f=ad-bc$ ，有

$$\alpha^2-e\alpha+f=0.$$

由 $\alpha=a+b\tau$ ，可得 $\mathbb{Q}(\tau)=\mathbb{Q}(\alpha)$ 是虚二次域，则 $\mathrm{End}(E)$ 同构于该域的整数环，而 E 带复乘，即 $\mathrm{End}(E)$ 大于 $\mathbb{Z}$ ，所以 $\mathrm{End}(E)$ 是该虚二次域的 order.

注意：有限域上非超奇异的椭圆曲线 E 的自同态环 $\mathrm{End}(E)$ 也同构于虚二次域的 order.

定理 6.1.8　设二次代数整数 τ 的虚部大于 0，则椭圆曲线 $E_\tau=\mathbb{C}/(\mathbb{Z}+\mathbb{Z}\tau)$ 带复乘，且 $\mathrm{End}(E_\tau)$ 同构于 $\mathbb{Q}(\tau)$ 的 order ， $j(E_\tau)=j(\tau)$ 是代数整数.

定理 6.1.9　设二次虚数 $\tau\in\mathcal{H}$ ，其判别式为 D ，则 $j(\tau)$ 是次数为 $h(D)$ 的代数整数，其中 $h(D)$ 是判别式 D 决定的虚二次 order 的类数，即 $j(\tau)$ 在 $\mathbb{Z}$ 上的极小多项式为

$$\prod(X-j(\alpha))=0,$$

其中，α 跑遍 D 的约化形式所决定的二次代数整数，二次虚数是指虚部大于 0 的二次代数整数.

定理 6.1.10　设椭圆曲线 E 的自同态环 $\mathrm{End}(E)$ 同构于判别式 D 决定的

虚二次 order， p 是素数，则

$$|E(\mathbb{F}_p)| = p + 1 - a_p,$$

其中， a_p 为：

(1) 若 $\left(\frac{D}{p}\right) = -1$ ，则 $a_p = 0$;

(2) 若 p 可以分解为两个素元的乘积，即 $p = \pi\tilde{\pi}$ ，则适当选择 π ，有 $a_p = \pi + \tilde{\pi}$.

注意：当 $D < -4$ 时，因为 order 中有 2 个可逆元，所以 π 有两种选择，其所决定的 a_p 分别对应于互扭的两条椭圆曲线；当 $D = -4$ 时， π 有 4 种选择；当 $D = -3$ 时， π 有 6 种选择. 以上内容请参阅文献 [18].

6.2 Goldwasser-Kilian 测试

设 N 是需要测试的整数， $\gcd(N, 6) = 1$ ，定义在 $\mathbb{Z}_N = \mathbb{Z}/N\mathbb{Z}$ 上的椭圆曲线

$$E : Y^2 = X^3 + aX + b,$$

则 $4a^3 + 27b^2 \in \mathbb{Z}_N^\times$. 对于 E 中点的加法运算依据 N 是素数计算，因为点加需要 $\mathbb{Z}_N$ 中的加法、减法、乘法和除法，所以加法运算无法进行，仅当对应的 $\mathbb{Z}_N$ 中除法无效，即某个元素 $c \in \mathbb{Z}_N$ ，在点加中作了分母，而其在 $\mathbb{Z}_N$ 中不可逆，故 c 与 N 不互素，则 N 是合数. 以下均假设 N 为素数执行运算，且运算均有效.

命题 6.2.1 设 $N \neq 1$ 是与 6 互素的正整数， E 是定义在 $\mathbb{Z}_N$ 上的椭圆曲线，若存在整数 m 和 E 在 $\mathbb{Z}_N$ 上的点 P 满足下述条件：

(1) 存在 m 的素因子 q, 使得 $q > (\sqrt[4]{N} + 1)^2$ ；

(2) $mP = O$ ；

(3) $\frac{m}{q}P = (x, y, t), t \in \mathbb{Z}_N^\times$.

则 N 是素数.

证明 若 N 不是素数，不妨设 p 是 N 的素因子，且 $p \leqslant \sqrt{N}$. 因为 $mP = O, t \in \mathbb{Z}_N^\times$ ，所以 $P \mod p$ 在 $E(\mathbb{F}_p)$ 中的阶 m_p 是 m 的因子，但不是 $\frac{m}{q}$ 的因子，而 q 是素数，故 $q | m_p$ ，进一步有 $q \leqslant |E(\mathbb{F}_p)|$ ，即

$$q \leqslant (\sqrt{p} + 1)^2 \leqslant (\sqrt[4]{N} + 1)^2,$$

与已知矛盾，所以 N 是素数.

要利用上述命题判定 N 是否为素数，需要解决 3 个问题，即选择椭圆曲线、选择点 P 及选择 m.

命题 6.2.2 设 N 是与 6 互素的素数，E 是定义在 $\mathbb{F}_N$ 上的椭圆曲线，令 $m=|E(\mathbb{F}_N)|$，若存在 m 的素因子 q，满足

$$q>(\sqrt[4]{N}+1)^2,$$

则存在 E 在 $\mathbb{F}_N$ 上的点 P，使得 $mP=O, \dfrac{m}{q}P\neq O$.

证明 因为 $m=|E(\mathbb{F}_N)|$，所以对于任意的 $P\in E(\mathbb{F}_N)$，均有 $mP=O$；若对于任意的 $P\in E(\mathbb{F}_N)$，还有 $\dfrac{m}{q}P=O$，则 P 的阶是 $\dfrac{m}{q}$ 的因子，由定理 2.9.1 知

$$E(\mathbb{F}_N)\simeq \mathbb{Z}_{n_1}\times\mathbb{Z}_{n_2}, n_1|n_2, n_1|N-1.$$

故 $n_2\Big|\dfrac{m}{q}$，则 $m\leqslant n_2^2\leqslant\left(\dfrac{m}{q}\right)^2$，所以 $q^2\leqslant m$，而 $m\leqslant(\sqrt{N}+1)^2$，故

$$(\sqrt[4]{N}+1)^4<q^2\leqslant m\leqslant(\sqrt{N}+1)^2,$$

矛盾，所以存在 $P\in E(\mathbb{F}_N)$，使得 $\dfrac{m}{q}P\neq O$.

对于给定的椭圆曲线 E，Goldwasser 和 Kilian 建议利用 Schoof 算法计算 E 的阶，因为 Schoof 算法是对素数有效的，故 Schoof 算法可能无效，这表明 N 是合数. 一旦确定了 $m=|E(\mathbb{Z}_N)|$，分解 m，希望 m 有满足命题要求的大素因子 q，Goldwasser 和 Kilian 要求 $q=m/2$ 是大伪素数. 若存在 q，假设 q 是素数，则随机选取 $P\in E(\mathbb{Z}_N)$，判断 P 是否满足命题 6.2.1 的条件，若满足，则只需证明 q 是素数，即将 N 的素性判断问题转化为

$$q\leqslant\frac{m}{2}\leqslant(N+2\sqrt{N}+1)/2$$

的素性判断问题，只需递归调用该算法 $O(\ln N)$ 次即可结束算法，当 N 较小时，可以利用试除法来判断 N 是否为素数. 总结以上，得如下算法.

算法 6.1 (Goldwasser-Kilian)

输入 正整数 $N\neq 1$ 且与 6 互素.

输出 1 表示 N 是合数，0 表示 N 是素数.

(1) 令 $i=0, N_i=N$；

(2) 若 $N_i < 2^{30}$，用试除法判断 N_i 是不是素数，若是，则输出 0，若不是，则转至第 (9) 步；

(3) 随机选择 $a, b \in \mathbb{Z}_{N_i}$，若 $4a^3 + 27b^2 \in \mathbb{Z}_{N_i}^{\times}$，则令 E 为 $Y^2 = X^3 + aX + b$；

(4) 利用 Schoof 算法计算 $|E(\mathbb{Z}_{N_i})|$，记作 m；若 Schoof 算法失效，转至第 (9) 步；

(5) 判断 m 是否存在大因子 $q > (\sqrt[4]{N_i} + 1)^2$，且 q 是强素数. 若不存在，则转至第 (3) 步；

(6) 随机选择 $x \in \mathbb{Z}_{N_i}$, 且满足 Legendre 符号 $\left(\dfrac{x^3 + ax + b}{N_i}\right) \neq -1$，计算 $y \in \mathbb{Z}_{N_i}, y^2 = x^3 + ax + b$，若 y 不存在，则转至第 (9) 步；

(7) 计算 $P_1 = mP, P_2 = \dfrac{m}{q}P$，若计算失效，则转至第 (9) 步，若 $P_1 \neq O$，则转至第 (9) 步；若 $P_2 = O$，则转至第 (6) 步；

(8) $i = i + 1, N_i = q$，转至第 (2) 步；

(9) 若 $i = 0$，输出 1；否则，令 $i = i - 1$，转至第 (3) 步.

该算法不会输出错误结果. 当 N 是合数时，该算法或者输出 1，或者永不停机；当 N 是素数时，因为算法利用了具有特殊性质的椭圆曲线，所以输出结果不一定正确，即其是概率算法. 文献 [43],[69] 对该算法的运行时间进行了分析，有以下结论.

定理 6.2.3 设存在正整数 c_1, c_2，使得 $[x, x+\sqrt{2x}] (x \geqslant 2)$ 间素数的个数大于 $c_1\sqrt{x}(\log x)^{-c_2}$，则对于整数 N，上述算法的期望运行时间为$O((\log N)^{10+c_2})$.

定理 6.2.4 存在正整数 c_3, c_4，使得对于任意的 $k \geqslant 2$，上述算法在期望运行时间 $c_3(\log N)^{11}$ 内可以判定的 k 比特素数 N 所占的比例至少为 $1 - c_4 2^{-k^{\frac{1}{\log\log k}}}$.

6.3 Atkin 测试

利用命题 6.2.1 和带复乘的椭圆曲线，Atkin 提出了一个实用的椭圆曲线素性判断算法，Atkin 和 Morain 实现了该算法并测试了 1000 位十进制数的素性. 其核心思想是若 N 可以分解为 O_K 中两个元素的乘积，其中 $K = \mathbb{Q}(\sqrt{D})$，则容易确定自同态环同构于其 order 的椭圆曲线 E，若 N 是素数，则利用定理 6.1.10 可以求得 $|E(\mathbb{Z}_N)|$. 从而可以舍弃算法 6.1 中利用 Schoof 算法求阶的过程.

以下均认为 N 是素数. 利用 Cornacchia 算法，可以求得 D，使得 N 在判

别式 D 决定的 order 中分裂为两个元素的乘积，实际上， Cornacchia 算法输出了 $X^2 - DY^2 = 4N$ 在 $\mathbb{Z}^2$ 中的一个解 (x, y) ，使得 $N = \pi\tilde{\pi}, \pi = \dfrac{x + y\sqrt{D}}{2}$. 由定理 6.1.10 知若椭圆曲线 E 的自同态环同构于判别式 D 所决定的 order ，则

$$m = |E(\mathbb{Z}_N)| = N + 1 - \pi - \tilde{\pi} = N + 1 - x.$$

然后检验 m 是否满足命题 6.2.1 的条件，若不满足，因为判别式 D 所决定的 order 中有 $\omega(D)$ 个单位根，所以定义在 $\mathbb{Z}_N$ 上且自同态环同构于 D 所决定的 order 的互不同构的椭圆曲线个数为 $\omega(D)$ ，其分别对应于 N 的不同分解，即 $N = (\zeta\pi)\widetilde{(\zeta\pi)}$ ，其中 ζ 跑遍所有的 $\omega(D)$ 次单位根. 故可以对 $\omega(D)$ 个不同的 m 判断是否满足命题 6.2.1 的条件，若均不满足，则选择另一个判别式. 若 m 满足条件，则需要确定 E 的方程：因为 N 在 D 的 order 中分裂，所以 $\omega(D)|N-1$ ，且存在 $\dfrac{N-1}{2}$ 个 $g \in \mathbb{Z}_N$(若 $D = -3$ ，则有 $\dfrac{N-1}{3}$ 个) 使得对于任意的素数 $p|\omega(D)$ ，有 $g^{\frac{N-1}{p}} \neq 1$. 选择其中之一记作 g.

若 $D = -4$ ，则自同态环同构于 -4 所决定的 order 且互不同构的 4 条椭圆曲线为

$$Y^2 \;=\; X^3 - g^k X, \qquad 0 \leqslant k \leqslant 3$$

若 $D = -3$ ，则自同态环同构于 -3 所决定的 order 且互不同构的 6 条椭圆曲线为

$$Y^2 \;=\; X^3 - g^k, \qquad 0 \leqslant k \leqslant 5$$

若 $D \neq -4, -3$ ，令

$$c = \frac{j}{j - 1728},$$
$$j = j\left(\frac{D + \sqrt{D}}{2}\right),$$

则自同态环同构于 D 所决定的 order 且互不同构的两条椭圆曲线为

$$Y^2 = X^3 - 3cg^{2k}X + 2cg^{3k}, \qquad k = 0, 1.$$

上述的 j 是复数. 由定理 6.1.9 知 j 是次数为 $h(D)$ 的代数整数. 若 N 是素数，N 分裂，则 j 在 $\mathbb{Z}[X]$ 中的极小多项式 T 在 $\mathbb{Z}_N[X]$ 中可以完全分解. 因为 T 在

$\mathbb{C}$ 中的根均是 $j\left(\frac{D+\sqrt{D}}{2}\right)$ 的共轭，对任意的根均可以利用上述方程确定互不同构的椭圆曲线的方程，所以令 j 是 T 在 $\mathbb{Z}_N$ 中的任意根即可.

椭圆曲线方程确定后，算法的运行便和 Goldwasser-Kilian 算法相同. 但还需要注意两个问题：对于给定的 m ， $\omega(D)$ 条椭圆曲线 E 哪一条的阶为 m 呢？随机选择 E 上的点 P ，若 $mP=O$ ，则认为 E 的阶为 m. 若 $h(D)$ 较大，则求 j 较难，故尽可能考虑 $h(D)$ 较小的判别式 $D.T$ 的系数随 $h(D)$ 快速增加，为了提高算法效率，可以利用 genus fiels 或 Weber 函数，有关内容请参看文献 [7,95]. 这里仅给出 Atkin 算法的核心思想，不涉及任何效率优化. 假设判别式 D 按 $h(D)$ 递增的顺序排列.

算法 6.2 (Cornacchia)

输入 素数 p ，负整数 $D \equiv 0,1 \mod 4$ ， $|D|<4p$.

输出 输出整数对 (x,y) 满足 $x^2+|D|y^2=4p$ ；若不存在满足条件的整数对，则输出 0.

(1) 若 $p=2, D+8$ 是平方数，则输出 $(\sqrt{D+8},1)$ ；若 $p=2, D+8$ 不是平方数，则输出 0；

(2) $k=\left(\frac{D}{p}\right)$ ，若 $k=-1$ ，输出 0；

(3) 求解整数 $0 \leqslant x_0 < p, x_0^2 \equiv D \mod p$ ，若 $x_0 \not\equiv D \mod 2$ ，令 $x_0=p-x_0$. 令 $a=2p, b=x_0, l=\lfloor 2\sqrt{p} \rfloor$ ；

(4) 若 $b>l$ ，令 $r=a \mod b, a=b, b=r$ ，转至第 (4) 步；

(5) 若 D 不整除 $4p-b^2$ ，或 $c=\frac{4p-b^2}{|D|}$ 不是平凡数，则输出 0；否则，输出 $(x,y)=(b,\sqrt{c})$. 令 $\Delta(\tau)=q\left(1+\sum_{n\geqslant 1}(-1)^n(q^{n(3n-1)/2}+q^{n(3n+1)/2})\right)^{24}$, $f(\tau)=\frac{\Delta(2\tau)}{\Delta(\tau)}$ ，则

$$j(\tau)=\frac{(256f(\tau)+1)^3}{f(\tau)}.$$

算法 6.3

输入 负整数 N.

输出 $j\left(\frac{D+\sqrt{D}}{2}\right)$ 在 $\mathbb{Z}[X]$ 中的极小多项式.

(1) $P=1, b=D \mod 2, B=\lfloor\sqrt{|D|/3}\rfloor$；

(2) $t=\dfrac{b^2-D}{4}, a=\max\{b,1\}$；

(3) 若 $a\nmid t$，则转至第 (4) 步；否则，计算 $j=j\left(\dfrac{-b+\sqrt{D}}{2a}\right)$. 若 $a=b$ 或 $a^2=t$ 或 $b=0$，则令 $P=P(X-j)$；否则，$P=P(X^2-2Re(j)X+|j|^2)$，其中 $Re(j)$ 表示 j 的实部，$|j|$ 为 j 的范数；

(4) 令 $a=a+1$，若 $a^2\leqslant t$，则转至第 (3) 步；

(5) 令 $b=b+2$，若 $b\leqslant B$，则转至第 (2) 步；否则，令 P 的各项系数为离自身最近的整数，输出 P.

算法 6.4 (Atkin)

输入 强素数 $N\neq 1$ 且和 6 互素.

输出 0 表示 N 是素数；1 表示 N 是合数.

(1) $i=0, n=0, N_i=N$；

(2) 若 $N_i<2^{30}$，用试除法判断 N_i 是不是素数，若是，则输出 0；若不是，则转至第 (14) 步；

(3) $n=n+1, D=D_n$. 若 $\dfrac{D}{N}\neq 1$，则转至第 (3) 步；否则，利用 Cornacchia 算法求 $X^2+|D|Y^2=4N$ 在 $\mathbb{Z}$ 中的解 (x,y)，若没有解，则转至第 (3) 步；

(4) 令 $m=N+1+x, N+1-x$(若 $D=-4$，m 还可以取为 $N+1+2y, N+1-2y$；若 $D=-3$，m 还可以取为 $N+1+(x+3y), N+1-(x+3y), N+1+(x-3y), N+1-(x-3y)$)，首先利用试除法 (至多至 1000000) 分解 m，然后利用 Pollard $p-1$ 算法分解 m；

(5) 若对于某一个 m，存在因子 $q>(\sqrt[4]{N_i}+1)^2$，且 q 是强素数，则转至第 (6) 步；否则，转至第 (3) 步；

(6) 若 $D=-4$，令 $a=-1, b=0$；若 $D=-3$，令 $a=0, b=-1$；否则，利用算法 6.3 获得 $j\left(\dfrac{D+\sqrt{D}}{2}\right)$ 在 $\mathbb{Z}[X]$ 中的极小多项式 T，令 j 是 $\bar{T}\equiv T \mod N_i$ 在 $\mathbb{Z}_{N_i}$ 中的根，则 $c=\dfrac{j}{j-1728} \mod N_i, a=-3c \mod N_i, b=2c \mod N_i$；

(7) 令 g 为模 N_i 的二次非剩余，若 $D=-3$，还要求 $g^{\frac{N_i-1}{3}}\neq 1 \mod N_i$；

(8) 随机选择 $x\in\mathbb{Z}_{N_i}$，且 $\left(\dfrac{x^3+ax+b}{N_i}\right)\neq -1$，计算 $y\in\mathbb{Z}_{N_i}$ 使得 $y^2=x^3+ax+b$，若无解，则转至第 (14) 步；令 $k=0$；

(9) 在曲线 $Y^2 = X^3 + aX + b$ 上计算 $P_2 = \frac{m}{q}P, P_1 = qP_2$ ，若计算失效，则转至第 (14) 步；若 $P_1 = O$ ，则转至第 (12) 步；

(10) $k = k + 1$. 若 $k \geqslant \omega(D)$ ，则转至第 (14) 步；若 $D < -4$ ，令 $a = ag^2, b = bg^3$ ，转至第 (8) 步；若 $D = -4$ ，令 $a = ag$ ，转至第 (8) 步；若 $D = -3$ ，令 $b = bg$ ，转至第 (8) 步.

(11) 随机选择 $x \in \mathbb{Z}_{N_i}$ ，且 $\left(\frac{x^3 + ax + b}{N_i}\right) \neq -1$ ，计算 $y \in \mathbb{Z}_{N_i}$ 使得 $y^2 = x^3 + ax + b$ ，若无解，则转至第 (14) 步；在曲线 $Y^2 = X^3 + aX + b$ 上计算 $P_2 = \frac{m}{q}P, P_1 = qP_2$ ，若计算失效，则转至第 (14) 步；若 $P_1 \neq O$ ，则转至第 (10) 步；

(12) 若 $P_2 = O$ ，则转至第 (11) 步；

(13) $i = i + 1, N_i = q$ ，转至第 (2) 步；

(14) 若 $i = 0$ ，输出 1 ；否则， $i = i - 1$ ，转至第 (3) 步.

第 7 章　椭圆曲线密码的快速实现

在安全和实用的双重要求之下，椭圆曲线密码的基域特征为大素数 p 或 2，其上的椭圆曲线为一般的椭圆曲线，故而本章仅讨论该条件下椭圆曲线密码体制所涉及的核心运算的快速实现，包括点加、倍点、标量乘法以及双标量乘法.

7.1　点加 $P+Q$ 和倍点 $2P$

仿射坐标下的点加和倍点运算均需要一次有限域上的求逆运算和几次乘法，如果有限域上的求逆和乘法相比，其花费的代价太大，则利用投射坐标执行点加和倍点是最好的选择.

7.1.1　投射坐标

本节将投射坐标的概念略做推广．设 K 是基域，c,d 是自然数，如下定义 K 上非零三元组集合 $K^3\backslash\{(0,0,0)\}$ 上的等价关系 $\sim$：

$(X_1,Y_1,Z_1)\sim(X_2,Y_2,Z_2)$，若存在 $\lambda\in K^\times$，使得 $X_1=\lambda^cX_2, Y_1=\lambda^dY_2, Z_1=\lambda Z_2$.

$(X,Y,Z)\in K^3\backslash\{(0,0,0)\}$ 所在的等价类记为

$$(X:Y:Z)=\{(\lambda^cX,\lambda^dY,\lambda Z):\lambda\in K^\times\}.$$

$(X:Y:Z)$ 称为投射点，(X,Y,Z) 是 $(X:Y:Z)$ 的代表元，所有投射点组成的集合记作 $\mathbb{P}(K)$. 显然 $(X:Y:Z)$ 中的任何元素均可作该等价类的代表元．特别，若 $Z\neq 0$，则 $(X/Z^c,Y/Z^d,1)$ 也是 $(X:Y:Z)$ 的代表元，且是唯一的 Z 坐标值为 1 的代表元，故投射点组成的集合

$$\mathbb{P}(K)^\times=\{(X:Y:Z):X,Y,Z\in K,Z\neq 0\}$$

和仿射点组成的集合

$$\mathbb{A}(K)=\{(x,y):x,y\in K\}$$

之间存在一一对应关系．无穷远点集合定义为

$$\mathbb{P}(K)^0=\{(X:Y:Z):X,Y,Z\in K,Z=0\}.$$

将 K 上的仿射椭圆曲线方程 E 中的 X, Y 分别用 $X/Z^c, Y/Z^d$ 替换，再消去分母，则可得 E 的投射方程. 显然，$\mathbb{A}(K)$ 中 E 上的点和 $\mathbb{P}(K)^\times$ 中 E 上的点之间有一一对应关系. $\mathbb{P}(K)^0$ 中 E 上的点称为 E 的无穷远点. 投射坐标下的点加和倍点公式，可以通过先将投射点转化为仿射点，利用仿射坐标的相应公式求得结果，再将其转化为投射点来获得.

7.1.2 椭圆曲线 $Y^2 = X^3 + aX + b$

设 K 的特征为大素数 p，其上的椭圆曲线 $E: Y^2 = X^3 + aX + b$，本小节考虑不同坐标下的加法和倍点实现效率.

(1) 标准投射坐标　$c = d = 1$，投射点 $(X:Y:Z), Z \neq 0$ 对应的仿射点为 $(X/Z, Y/Z)$，椭圆曲线的投射方程为

$$Y^2Z = X^3 + aXZ^2 + bZ^3.$$

无穷远点为 $(0:1:0)$，$(X:Y:Z)$ 的负元为 $(X:-Y:Z)$.

(2) Jacobian 坐标　$c = 2, d = 3$，投射点 $(X:Y:Z), Z \neq 0$ 对应的仿射点为 $(X/Z^2, Y/Z^3)$，椭圆曲线的投射方程为

$$Y^2 = X^3 + aXZ^4 + bZ^6.$$

无穷远点为 $(1:1:0)$，$(X:Y:Z)$ 的负元为 $(X:-Y:Z)$，设

$$P = (X_1 : Y_1 : Z_1) \in E,$$
$$Q = (X_2 : Y_2 : 1) \in E,$$

其中 $Z_1 \neq 0, P \neq \pm Q$，则

$$2P = (X_3, Y_3, Z_3),$$
$$P + Q = (X_4, Y_4, Z_4),$$

其中

$$X_3 = (3X_1^2 + aZ_1^4)^2 - 8X_1Y_1^2,$$
$$Y_3 = (3X_1^2 + aZ_1^4)(4X_1Y_1^2 - X_3) - 8Y_1^4,$$
$$Z_3 = 2Y_1Z_1,$$
$$X_4 = (Y_2Z_1^3 - Y_1)^2 - (X_2Z_1^2 - X_1)^2(X_1 + X_2Z_1^2),$$

$$Y_4 = (Y_2Z_1^3 - Y_1)(X_1(X_2Z_1^2 - X_1)^2 - X_3) - Y_1(X_2Z_1^2 - X_1)^3,$$
$$Z_4 = (X_2Z_1^2 - X_1)Z_1.$$

点加的运算量为 3 次有限域的平方运算和 8 次乘法，倍点的运算量为 6 次平方和 4 次乘法. 若 $a = -3$ ，则

$$3X_1^2 + aZ_1^4 = 3(X_1 - Z_1^2)(X_1 + Z_1^2),$$

故倍点的运算量可减少为 4 次平方和 4 次乘法. 由于椭圆曲线之间存在同构关系，如果 $p \equiv 1 \mod 4$ ，那么有 1/4 的概率可以对椭圆曲线作同构变换，使得 $a = -3$ ；如果 $p \equiv 3 \mod 4$ ，那么有 1/2 的概率可以对椭圆曲线作同构变换，使得 $a = -3$ ，因此，该情况在密码体制实现中是很有意义的.

算法 7.1 (倍点： $Y^2 = X^3 - 3X + b$,Jacobian 坐标)

输入 $P = (X_1 : Y_1 : Z_1)$.

输出 $2P = (X_3 : Y_3 : Z_3)$.

(1) 若 $Z_1 = 0$ ，则返回 $(1 : 1 : 0)$;

(2) $T_1 \longleftarrow Z_1^2$;

(3) $T_2 \longleftarrow X_1 - T_1$;

(4) $T_1 \longleftarrow X_1 + T_1$;

(5) $T_2 \longleftarrow T_2 \cdot T_1$;

(6) $T_2 \longleftarrow 3T_2$;

(7) $Y_3 \longleftarrow 2Y_1$;

(8) $Z_3 \longleftarrow Y_3 \cdot Z_1$;

(9) $Y_3 \longleftarrow Y_3^2$;

(10) $T_3 \longleftarrow Y_3 \cdot X_1$;

(11) $Y_3 \longleftarrow Y_3^2$;

(12) $Y_3 \longleftarrow Y_2/2$;

(13) $X_3 \longleftarrow T_2^2$;

(14) $T_1 \longleftarrow 2T_3$;

(15) $X_3 \longleftarrow X_3 - T_1$;

(16) $T_1 \longleftarrow T_3 - X_3$;

(17) $T_1 \longleftarrow T_1 \cdot T_2$;

(18) $Y_3 \longleftarrow T_1 - Y_3$;

(19) 返回 $(X_3:Y_3:Z_3)$.

算法 7.2 (点加: $Y^2=X^3-3X+b$, 仿射 Jacobian 坐标)

输入 $P=(X_1,Y_1,Z_1), Q=(X_2,Y_2)$.

输出 $P+Q=(X_3:Y_3:Z_3)$.

(1) 若 $Z_1=0$，则返回 $(X_2,Y_2,1)$;

(2) $T_1 \longleftarrow Z_1^2$;

(3) $T_2 \longleftarrow T_1 \cdot Z_1$;

(4) $T_1 \longleftarrow T_1 \cdot X_2$;

(5) $T_2 \longleftarrow T_2 \cdot Y_2$;

(6) $T_1 \longleftarrow T_1 - X_1$;

(7) $T_2 \longleftarrow T_2 - Y_1$;

(8) 若 $T_1=0$，则:

①若 $T_2=0$，则调用算法 7.1 计算 $(X_3:Y_3:Z_3)=2(X_2:Y_2:1)$，返回 $(X_3:Y_3:Z_3)$;

②否则，返回 $(1:1:0)$；

(9) $Z_3 \longleftarrow Z_1 \cdot T_1$;

(10) $T_3 \longleftarrow T_1^2$;

(11) $T_4 \longleftarrow T_3 \cdot T_1$;

(12) $T_3 \longleftarrow T_3 \cdot X_1$;

(13) $T_1 \longleftarrow 2T_3$;

(14) $X_3 \longleftarrow T_2^2$;

(15) $X_3 \longleftarrow X_3 - T_1$;

(16) $X_3 \longleftarrow X_3 - T_4$;

(17) $T_3 \longleftarrow T_3 - X_3$;

(18) $T_3 \longleftarrow T_3 \cdot T_2$;

(19) $T_4 \longleftarrow T_4 \cdot Y_1$;

(20) $Y_3 \longleftarrow T_3 - T_4$;

(21) 返回 $(X_3:Y_3:Z_3)$.

不同坐标下点加和倍点所需的域操作个数请见表 7.1. 由表可知， Jacobian 坐标下倍点速度最快，而 Jacobian 仿射坐标下点加速度最快. 表中 A,P,J 分别为仿射坐标、标准投射坐标、 Jacobian 坐标， I,M,S 分别表示求逆、乘法、平

方的运行时间，$C_1+C_2 \to C_3$ 表示 C_1 坐标下的点与 C_2 坐标下的点相加，其和点为 C_3 坐标下的点.

表 7.1　域操作个数

倍点		点加	
$2A \to A$	$1I, 2M, 2S$	$A+A \to A$	$1I, 2M, 1S$
$2P \to P$	$7M, 3S$	$P+P \to P$	$12M, 2S$
$2J \to J$	$4M, 4S$	$J+J \to J$	$12M, 4S$
		$J+A \to J$	$8M, 3S$

7.1.3　椭圆曲线 $Y^2+XY=X^3+aX^2+b$

设 K 的特征为 2， $E: Y^2+XY=X^3+aX^2+b$ 为 K 上的椭圆曲线，本小节分析不同坐标下的点加和倍点的实现效率.

(1) 标准投射坐标　$c=d=1$，投射点 $(X:Y:Z), Z\neq 0$ 对应于仿射点 $(X/Z, Y/Z)$，椭圆曲线的投射方程为

$$Y^2+XYZ=X^3+aX^2Z+bZ^3.$$

无穷远点为 $(0:1:0)$， $(X:Y:Z)$ 的负元为 $(X:X+Y:Z)$.

(2) Jacobian 坐标　$c=2, d=3$，投射点 $(X:Y:Z), Z\neq 0$ 对应于仿射点 $(X/Z^2, Y/Z^3)$，椭圆曲线的投射方程为

$$Y^2+XYZ=X^3+aX^2Z^2+bZ^6.$$

无穷远点为 $(1:1:0)$， $(X:Y:Z)$ 的负元为 $(X:X+Y:Z)$.

(3) López-Dahab(LD) 坐标　$c=1, d=2$，投射点 $(X:Y:Z), Z\neq 0$ 对应于仿射点 $(X/Z, Y/Z^2)$，椭圆曲线的投射方程为

$$Y^2+XYZ=X^3Z+aX^2Z^2+bZ^4.$$

无穷远点为 $(1:0:0)$， $(X:Y:Z)$ 的负元为 $(X:X+Y:Z)$. 设 $P=(X_1:Y_1:Z_1), Q=(X_2:Y_2:1)$，则 $2P=(X_3:Y_3:Z_3), P+Q=(X_4:Y_4:Z_4)$，其中

$$Z_3=X_1^2\cdot Z_1^2;$$

$$X_3=X_1^4+b\cdot Z_1^4;$$

$$Y_3 = bZ_1^4 \cdot Z_3 + X_3 \cdot (aZ_3 + Y_1^2 + bZ_1^4);$$
$$A = Y_2 Z_1^2 + Y_1;$$
$$B = X_2 Z_1 + X_1;$$
$$C = Z_1 B;$$
$$D = B^2(C + aZ_1^2);$$
$$Z_4 = C^2;$$
$$E = AC;$$
$$X_4 = A^2 + D + E;$$
$$F = X_3 + X_2 Z_3;$$
$$G = (X_2 + Y_2) Z_3^2;$$
$$Y_4 = (E + Z_3)F + G.$$

由于 $a \in \{0,1\}$ 时，点加和倍点均可以减少一次乘法，而对椭圆曲线 $E: Y^2 + XY = X^3 + aX^2 + b$ 作坐标变换

$$X' = X,$$
$$Y' = Y + dX,$$

其中 $d^2 + d + a = \mathrm{Tr}(a)$，即得 E 的同构曲线

$$E' : Y'^2 + X'Y' = X'^3 + a'X^2 + b'.$$

其中，$a' \in \{0,1\}$，故不妨假定 $a \in \{0,1\}$.

算法 7.3 (倍点： $Y^2 + XY = X^3 + aX^2 + b, a \in \{0,1\}$, LD 坐标)

输入 $P = (X_1 : Y_1 : Z_1)$.

输出 $2P = (X_3 : Y_3 : Z_3)$.

(1) 若 $Z_1 = 0$，则返回 $(1:0:0)$;

(2) $T_1 \longleftarrow Z_1^2$;

(3) $T_2 \longleftarrow X_1^2$;

(4) $Z_3 \longleftarrow T_1 \cdot T_2$;

(5) $X_3 \longleftarrow T_2^2$;

(6) $T_1 \longleftarrow T_1^2$;

(7) $T_2 \longleftarrow T_1 \cdot b$;

(8) $X_3 \longleftarrow X_3 + T_2$;

(9) $T_1 \longleftarrow Y_1^2$;

(10) 若 $a=1$，则 $T_1 \longleftarrow T_1 + Z_3$;

(11) $T_1 \longleftarrow T_1 + T_2; Y_3 \longleftarrow X_3 \cdot T_1$;

(12) $T_1 \longleftarrow T_2 \cdot Z_3; Y_3 \longleftarrow Y_3 + T_1$;

(13) 返回 $(X_3 : Y_3 : Z_3)$.

算法 7.4 (点加: $Y^2 + XY = X^3 + aX^2 + b, a \in \{0,1\}$,LD 仿射坐标)

输入 $P = (X_1 : Y_1 : Z_1), Q = (X_2, Y_2)$.

输出 $P + Q = (X_3 : Y_3 : Z_3)$.

(1) 若 $Z_1 = 0$，则返回 $(X_2 : Y_2 : 1)$;

(2) $T_1 \longleftarrow Z_1 \cdot X_2$;

(3) $T_2 \longleftarrow Z_1^2$;

(4) $X_3 \longleftarrow X_1 + T_1$;

(5) $T_1 \longleftarrow Z_1 \cdot X_3$;

(6) $T_3 \longleftarrow T_2 \cdot Y_2$;

(7) $Y_3 \longleftarrow Y_1 + T_3$;

(8) 若 $X_3 = 0$，则:

①若 $Y_3 = 0$，调用算法 7.3 计算 $(X_3 : Y_3 : Z_3) = 2(X_2 : Y_2 : 1)$ 并返回 $(X_3 : Y_3 : Z_3)$;

②否则返回 $(1 : 0 : 0)$;

(9) $Z_3 \longleftarrow T_1^2$;

(10) $T_3 \longleftarrow T_1 \cdot Y_3$;

(11) 若 $a=1$，则 $T_1 \longleftarrow T_1 + T_2$;

(12) $T_2 \longleftarrow X_3^2$;

(13) $X_3 \longleftarrow T_2 \cdot T_1$;

(14) $T_2 \longleftarrow Y_3^2$;

(15) $X_3 \longleftarrow X_3 + T_2$;

(16) $X_3 \longleftarrow X_3 + T_3$;

(17) $T_2 \longleftarrow X_2 \cdot Z_3$;

(18) $T_2 \longleftarrow T_2 + X_3$;

(19) $T_1 \longleftarrow Z_3^2$;

(20) $T_3 \longleftarrow T_3 + Z_3$;

(21) $Y_3 \longleftarrow T_3 \cdot T_2$;

(22) $T_2 \longleftarrow X_2 + Y_2$;

(23) $T_3 \longleftarrow T_1 \cdot T_2$;

(24) $Y_3 \longleftarrow Y_3 + T_3$;

(25) 返回 $(X_3 : Y_3 : Z_3)$.

在不同坐标下，倍点和点加所需的运算量请见表 7.2. 表中 A, P, J, L 分别为仿射坐标、标准投射坐标、 Jacobian 坐标和 LD 坐标.

表 7.2 倍点和点加所需的运算量

倍点		点加	
$2P \to P$	$7M$	$P + P \to P$	$13M$
$2J \to J$	$5M$	$J + J \to J$	$14M$
$2L \to L$	$4M$	$L + L \to L$	$14M$
		$P + A \to P$	$12M$
		$J + A \to J$	$10M$
		$L + A \to L$	$8M$

7.2 标量乘法 kP

7.2.1 动点的标量乘法

椭圆曲线点的标量乘法 kP 是普通 Abel 群模指数运算的特殊情况，因此，针对指数运算的各种方法和技巧都可以应用到椭圆曲线点的标量乘法中. 最简单的指数运算算法是二进制方法，设指数 $k = \sum\limits_{j=0}^{l-1} k_j 2^j, k_j \in \{0, 1\}$ ，则共需 l 次倍点运算和 $\sum\limits_{j=0}^{l-1} k_j$ 次点加运算.

椭圆曲线群作为特殊的 Abel 群，其上两点相加和两点相减所需的运算量相同，因此可以对指数重新编码以减少二进制方法中点加次数. 设

$$k = \sum_{i=0}^{l-1} k_i 2^i, \qquad k_i \in \{0, -1, 1\},$$

则称 $(k_{l-1},\cdots,k_1,k_0)_2$ 为 k 的有符号二进制表示，不妨记 $-1=\bar{1}$. 显然，任何整数都可以表示成有符号二进制串，而且其表示不是唯一的. 若

$$k=\sum_{i=0}^{t-1}k_i2^i,\qquad k_i\in\{0,\pm1,\pm3,\cdots,\pm(2^{w-1}-1)\},$$

其中 w 是正整数，则称 $(k_{t-1},\cdots,k_1,k_0)_w$ 为 w 窗口的广义二进制表示，记作 GF_w. 重新编码的目的是以有符号二进制表示来减少二进制表示中非零元个数. 如果一个有符号位向量 $(k_{l-1},\cdots,k_1,k_0)_2, k_{l-1}\neq 0$ ，没有相邻的非零元素，则称其为非相邻有符号二进制表示 (non-adjacent form,NAF). 可以证明，对每个整数 k ，存在唯一的 NAF ，而且在 k 的所有有符号二进制表示中， NAF 具有最小的 Hamming 重量 (非零元个数)，其长度至多比最短的有符号二进制表示多一比特，该表示记作 NAF(k).

算法 7.5 (NAF 编码)

输入 正整数 k.

输出 NAF(k).

(1) $i\longleftarrow 0$;

(2) While $k\geqslant 1$ do

①若 k 为奇数，则 $k_i\longleftarrow 2-(k \mod 4), k\longleftarrow k-k_i$;

②否则 $k_i\longleftarrow 0$;

③ $k\longleftarrow k/2, i\longleftarrow i+1$;

(3) 返回 $(k_{i-1},k_{i-2},\cdots,k_1,k_0)$.

设 A,D 分别表示一次点加、倍点的运行时间，则利用 NAF 表示实现标量乘法 kP 的运行时间约为 $\frac{m}{3}A+mD$ ，其中 $m=\lceil\log_2 k\rceil$.

算法 7.6 (NAF 标量乘法)

输入 正整数 k ，点 P.

输出 kP.

(1) 调用算法 7.5 计算 NAF$(k)=\sum_{i=0}^{l-1}k_i2^i$;

(2) Q 为无穷远点;

(3) For i from $l-1$ downto 0 do

① $Q\longleftarrow 2Q$;

②若 $k_i=1$ ，则 $Q\longleftarrow Q+P$;

③若 $k_i = -1$ ，则 $Q \longleftarrow Q - P$ ；

(4) 返回 Q.

如果允许存储少量数据，则可以将 NAF 和广义二进制表示相结合，对指数重新编码，减少点加次数，进而提高标量乘法的效率．整数 k 的 w 窗口 NAF 编码是 $k = \sum_{i=0}^{l-1} k_i 2^i$ ，其中非零的 k_i 均为奇数， $|k_i| < 2^{w-1}$ ，且任意 w 个连续项中至多有一个为非零，该编码记作 $\mathrm{NAF}_w(k)$．可以证明 $\mathrm{NAF}_w(k)$ 的长度和最短的 $\mathrm{GF}_w(k)$ 的长度之差最大为 1 ， l 长的 w 窗口 NAF 编码的 Hamming 重量期望值为 $l/(w+1)$.

算法 7.7 (NAF_w 编码)

输入 正整数 k, w.

输出 $\mathrm{NAF}_w(k)$.

(1) $i \longleftarrow 0$;

(2) While $k \geqslant 1$ do

①若 k 是奇数，则 $k_i \longleftarrow k \bmod\mathrm{s}\ 2^w, k \longleftarrow k - k_i$, 其中 $k \bmod\mathrm{s}\ 2^w$ 是指 $-2^{w-1}, 2^{w-1}$ 之间与 k 模 2^w 同余的值;

②否则 $k_i \longleftarrow 0$;

③ $k \longleftarrow k/2, i \longleftarrow i+1$;

(3) 返回 $(k_{i-1}, k_{i-2}, \cdots, k_1, k_0)$.

显然，算法 7.6 中的 NAF(k) 可以用 $\mathrm{NAF}_w(k)$ 替换，从而得到算法 7.8 ，其运行时间约为

$$[1D + (2^{w-2} - 1)A] + \left[\frac{m}{w+1}A + mD\right].$$

算法 7.8 (NAF_w 标量乘法)

输入 正整数 k, w ，点 P.

输出 kP.

(1) 调用算法 7.7 计算 $\mathrm{NAF}_w(k) = \sum_{i=0}^{l-1} k_i 2^i$;

(2) 计算 $P_i = iP, i \in \{1, 3, 5, \cdots, 2^{w-1} - 1\}$;

(3) Q 为无穷远点;

(4) For i from $l-1$ downto 0 do;

① $Q \longleftarrow 2Q$;

②若 $k_i > 0$，则 $Q \longleftarrow Q + P_{k_i}$;

③若 $k_i < 0$，则 $Q \longleftarrow Q - P_{-k_i}$;

(5) 返回 Q.

算法 7.8 实际上可以看作是 w 宽的窗口由左向右移动，直至遇到非零的 k_i 才操作. 依据该思想，对 NAF(k) 利用滑动窗口即得算法 7.9. 为了减少预计算，窗口 (其最大宽度为 w) 由 NAF(k) 的最左边向右移动，直至窗口所在二进制表示对应的数为奇数时才操作.

算法 7.9 (标量乘法的滑动窗口法)

输入 w, k 和点 P.

输出 kP.

(1) 调用算法 7.5 计算 $\text{NAF}(k) = \sum_{i=0}^{l-1} k_i 2^i$;

(2) 对于 $i \in \{1, 3, \cdots, 2(2^w - (-1)^w)/3 - 1\}$，计算 $P_i = iP$;

(3) Q 为无穷远点，$i \longleftarrow l - 1$;

(4) While $i \geqslant 0$ do;

①若 $k_i = 0$，则 $t \longleftarrow 1, u \longleftarrow 0$;

②否则，寻找满足 $t \leqslant w$ 且 $u \longleftarrow (k_i, \cdots, k_{i-t+1})$ 为奇数的最大的 t;

③ $Q \longleftarrow 2^t Q$;

④若 $u > 0$，则 $Q \longleftarrow Q + P_u$；若 $u < 0$，则 $Q \longleftarrow Q - P_{-u}$;

⑤ $i \longleftarrow i - t$;

(5) 返回 Q.

窗口间零比特的平均长度为

$$v(w) = \frac{4}{3} - \frac{(-1)^w}{3 \cdot 2^{w-2}}.$$

故算法 7.9 的运行时间约为

$$\left[1D + \left(\frac{2^w - (-1)^w}{3} - 1\right) A\right] + \frac{m}{w + v(w)} A + mD.$$

设 $E: Y^2 + XY = X^3 + aX^2 + b$ 是特征为 2 的有限域上的非超奇异椭圆曲线，基于 Montgomery 的思想 López 和 Dahab 给出了算法 7.10. 设 E 上的点 $Q_1 = (x_1, y_1), Q_2 = (x_2, y_2), Q_1 \neq \pm Q_2, Q_1 + Q_2 = (x_3, y_3), Q_1 - Q_2 = (x_4, y_4)$，则

$$x_3 = x_4 + \frac{x_2}{x_1 + x_2} + \left(\frac{x_2}{x_1 + x_2}\right)^2.$$

即已知 x_1, x_2, x_4 便可以快速求得 x_3. 设 E 上的点 $P=(x,y), kP=(x_1,y_1),(k+1)P=(x_2,y_2)$，$k$ 的二进制表示的最低 j 比特决定的整数为 l，令 $T_j=\{lP,(l+1)P\}$，计算并存储 T_j 中各点的 X 坐标; 若其后的比特为 0，则

$$T_{j+1}=\{2lP,(2l+1)P=lP+(l+1)P\};$$

若其后的比特为 1，则

$$T_{j+1}=\{(2l+1)P,(2l+2)P=2(l+1)P\},$$

即每向右移动 1 比特，只需做一次倍点和一次点加; 最后，当移动到 k 的最右边时，求得 $kP,(k+1)P$ 的 X 坐标值，则

$$y_1=x^{-1}(x_1+x)[(x_1+x)(x_2+x)+x^2+y]+y.$$

算法 7.10 利用了标准投射坐标，在算法的第 (1) 、 (2) 步仅需要求取点的 X,Z 坐标值. 该算法没有额外的存储需求，而且循环体中每步操作相同，从而具有较好的抗时间攻击、能量攻击的能力; 其运行时间约为 $6mM+(1I+10M)$.

算法 7.10 (Montgomery 标量乘法: $\mathbb{F}_{2^t}$ 上的椭圆曲线)

输入 k 的二进制表示为 $(k_{m-1},\cdots,k_1,k_0)_2, k_{m-1}=1, P=(x,y)$.

输出 kP.

(1) $X_1 \longleftarrow x, Z \longleftarrow 1, X_2 \longleftarrow x^4+b, Z_2 \longleftarrow x^2$;

(2) For i from $m-2$ downto 0 do

①若 $k_i=1$ 则

$T \longleftarrow Z_1, Z_1 \longleftarrow (X_1Z_2+X_2Z_1)^2, X_1 \longleftarrow xZ_1+X_1X_2TZ_2$;

$T \longleftarrow X_2, X_2 \longleftarrow X_2^4+bZ_2^4, Z_2 \longleftarrow T^2Z_2^2$;

②否则

$T \longleftarrow Z_2, Z_2 \longleftarrow (X_1Z_2+X_2Z_1)^2, X_2 \longleftarrow xZ_2+X_1X_2Z_1T$;

$T \longleftarrow X_1, X_1 \longleftarrow X_1^4+bZ_1^4, Z_1 \longleftarrow T^2Z_1^2$;

(3) $x_3 \longleftarrow X_1/Z_1$;

(4) $y_3 \longleftarrow (x+X_1/Z_1)[(X_1+xZ_1)(X_2+xZ_2)+(x^2+y)(Z_1Z_2)](xZ_1Z_2)^{-1}+y$;

(5) 返回 (x_3,y_3).

7.2.2 定点的标量乘法

若点 P 是固定的且允许存储，则通过预计算一些与 P 相关的值，可以提高 kP 的实现速度.

算法 7.11 是 Brickell, Gordon, McCurley 和 Wilson 提出的. 设 $(K_{d-1},\cdots,K_1,K_0)_{2^w}$ 是 k 的基为 2^w 的表示，其中 $d=\lceil m/w\rceil$ ，令 $Q_j=\sum\limits_{i:K_i=j}2^{wi}P, 1\leqslant j\leqslant 2^w-1$ ，则

$$
\begin{aligned}
kP &= \sum_{i=0}^{d-1}K_i(2^{wi}P)=\sum_{j=1}^{2^w-1}\left(j\sum_{i:K_i=j}2^{wi}P\right)=\sum_{j=1}^{2^w-1}jQ_j\\
&= Q_{2^w-1}+(Q_{2^w-1}+Q_{2^w-2})+\cdots+(Q_{2^w-1}+Q_{2^w-2}+\cdots+Q_1).
\end{aligned}
$$

上式便是算法 7.11 的核心思想，该算法的运行时间约为 $(2^w+d-3)A$.

算法 7.11 (标量乘法的固定基窗口算法)

输入 $w, d=\lceil m/w\rceil, k=(K_{d-1},\cdots,K_1,K_0)_{2^w}$ 及点 P.

输出 kP.

(1) 预计算： $P_i=2^{wi}P, 0\leqslant i\leqslant d-1$;

(2) A, B 均为无穷远点;

(3) For j from 2^w-1 downto 1 do

① 对于每一个 i ，若 $K_i=j$ ，则 $B\longleftarrow B+P_i$;

② $A\longleftarrow A+B$;

(4) 返回 A.

若用 NAF(k) 代替 k 的二进制表示，即将 NAF(k) 分为若干个 $\{0,\pm1\}$ 串 K_i 且每个 K_i 的长度均为 w ：

$$\mathrm{NAF}(k)=K_{d-1}||\cdots||K_1||K_0.$$

因为 K_i 为非相邻有符号二进制串，所以其表示范围为 $[-I,I]$ ，其中当 w 是偶数时， $I=(2^{w+1}-2)/3$ ；当 w 是奇数时， $I=(2^{w+1}-1)/3$. 将该思想用于算法 7.11 即得算法 7.12 ，其运行时间约为

$$\left(\frac{2^{w+1}}{3}+d-2\right)A.$$

其中， $d=\lceil (m+1)/w\rceil$.

算法 7.12 (标量乘法的固定基 NAF 窗口算法)

输入 w, k 和点 P.

输出 kP.

(1) 预计算: $P_i = 2^{wi}P, 0 \leqslant i \leqslant \lceil (m+1)/w \rceil$;

(2) 调用算法 7.5 计算 $\mathrm{NAF}(k) = \sum\limits_{i=0}^{l-1} k_i 2^i$;

(3) $d \longleftarrow \lceil l/w \rceil$;

(4) 若需要, 可在 NAF(k) 的左边填充 0，令 $(k_{l-1}, \cdots, k_1, k_0) = K_{d-1}||\cdots||K_1||K_0$，其中 K_i 均为长 w 的 $\{0, \pm 1\}$ 串;

(5) 若 w 是偶数, 则 $I \longleftarrow (2^{w+1}-2)/3$；否则 $I \longleftarrow (2^{w+1}-1)/3$;

(6) A, B 为无穷远点;

(7) For j from i downto 1 do

①对于每个 i，若 $K_i = j$，则 $B \longleftarrow B + P_i$;

②对于每个 i，若 $K_i = -j$，则 $B \longleftarrow B - P_i$;

③ $A \longleftarrow A + B$;

(8) 返回 A.

设 $d = \lceil m/w \rceil$，在 k 的二进制表示的左边填充 $dw - m$ 个 0，并将其分为 d 长的 w 个比特串:

$$k = K^{w-1}||\cdots||K^1||K^0.$$

比特串 K^j 可作为指数阵列的行向量, 即

$$\begin{bmatrix} K^0 \\ \vdots \\ K^{w'} \\ K^{w-1} \end{bmatrix} = \begin{bmatrix} K^0_{d-1} & & K^0_0 \\ \vdots & & \vdots \\ K^{w'}_{d-1} & & K^{w'}_0 \\ \vdots & & \vdots \\ K^{w-1}_{d-1} & \cdots & K^{w-1}_0 \end{bmatrix} = \begin{bmatrix} k_{d-1} & k_0 \\ \vdots & \vdots \\ k_{(w'+1)d-1} & k_{w'd} \\ \vdots & \vdots \\ k_{wd-1} & k_{(w-1)d} \end{bmatrix}.$$

其列向量作为整体处理, 则对于所有可能的比特串 $(a_{w-1}, \cdots, a_1, a_0)$，必须预计算

$$[a_{w-1}, \cdots, a_1, a_0]P = a_{w-1}2^{(w-1)d}P + \cdots + a_2 2^{2d}P + a_1 2^d P + a_0 P.$$

在求取 kP 时, 循环体的每步操作处理一列, 从而提高实现效率.

算法 7.13 (标量乘法的固定梳形算法)

输入 $w, d=\lceil m/w \rceil, k$ 的二进制表示 $(k_{m-1}, \cdots, k_1, k_0)$ 和点 P.

输出 kP.

(1) 预计算：对于所有的比特串 $(a_{w-1}, \cdots, a_1, a_0)$，计算 $[a_{w-1}, \cdots, a_1, a_0]P$;

(2) 若需要，则在 k 的左边填充 0，令 $k=K^{w-1}||\cdots||K^1||K^0$，其中 K^j 是 d 长的比特串，K_i^j 表示 K^j 的第 i 比特;

(3) Q 为无穷远点;

(4) For i from $d-1$ downto 0 do

① $Q \longleftarrow 2Q$;

$Q \longleftarrow Q+[K_i^{w-1}, \cdots, K_i^1, K_i^0]P$;

(5) 返回 Q.

算法 7.13 的运行时间约为

$$\left(\frac{2^w-1}{2^w}d-1\right)A+(d-1)D.$$

若 $w>2$，则该算法在循环体中倍点和点加的次数相当. 与此相比，带表的固定梳形算法增加了预计算的数据量，但循环体中的每次操作可以同时处理多列，从而减少循环体中倍点的次数，提高标量乘法的实现速度. 算法 7.14 是双表的固定梳形算法，其倍点次数仅是点加次数的一半.

算法 7.14 (标量乘法的双表固定梳形算法)

输入 $w, d=\lceil m/w \rceil, e=\lceil d/2 \rceil, k=(k_{m-1}, \cdots, k_0), k_i \in \{0,1\}$ 和点 P.

输出 kP.

(1) 预计算：对于所有的 $(a_{w-1}, \cdots, a_1, a_0)$，计算 $[a_{w-1}, \cdots, a_1, a_0]P$, $2^e[a_{w-1}, \cdots, a_1, a_0]P$;

(2) 若需要，则在 k 的左边填充 0，令 $k=K^{w-1}||\cdots||K^1||K^0$，其中 K^j 是 d 长的比特串，K_i^j 表示 K^j 的第 i 比特;

(3) Q 为无穷远点;

(4) For i from $e-1$ downto 0 do

① $Q \longleftarrow 2Q$;

② $Q \longleftarrow Q+[K_i^{w-1}, \cdots, K_i^1, K_i^0]P+2^e[K_{i+e}^{w-1}, \cdots, K_{i+e}^1, K_{i+e}^0]P$;

(5) 返回 Q.

算法 7.14 的运行时间约为

$$\left(\frac{2^w-1}{2^w}2e-1\right)A+(e-1)D.$$

给定 w，则当算法 7.14 的预计算量是算法 7.13 的两倍；给定预计算量，则当

$$\frac{2^{w-1}(w-1)}{2^w-w-1} \geqslant \frac{A}{D}$$

时，算法 7.14 优于算法 7.13，其中 w 是算法 7.13 的窗口宽度. 如果 LD 坐标下 $A/D \approx 2$，则算法 7.13 中的 $w \geqslant 6$ 时，双表梳形算法较优.

7.3 双标量乘法 $kP+lQ$

7.3.1 JSF

在椭圆曲线密码体制中，特别是椭圆曲线数字签名体制的验证过程中，需要计算 $kP+lQ$，其中 P,Q 是椭圆曲线上的点，故椭圆曲线密码体制的快速实现依赖于双标量乘法的快速实现.

Shamir 算法通过对 kP,lQ 做同步处理以加速求取 $kP+lQ$. 设 k,l 是 t 比特长的整数，则 k,l 可以表示为 $2\times t$ 的矩阵，称为指数阵列. 给定窗口 w，对于所有的 $0\leqslant i,j<2^w$，预计算 $iP+jQ$，则需要存储 $2^{2w}-1$ 个点；求取 $kP+lQ$ 时，共需要 $\lceil t/w\rceil$ 次循环，每次循环执行 w 次倍点和一次加法，其运行时间约为

$$[(3\cdot 2^{2(w-1)}-2^{w-1}-1)A+(2^{2(w-1)}-2^{w-1})D]+\left[\left(\frac{2^{2w}-1}{2^{2w}}d-1\right)A+(d-1)wD\right].$$

算法 7.15 (Shamir 算法)

输入 $w,k=(k_{t-1},\cdots,k_0),l=(l_{t-1},\cdots,l_0),k_i\in\{0,1\},l_i\in\{0,1\}$ 和点 P,Q.

输出 $kP+lQ$.

(1) 预计算：对于所有的 $0\leqslant i,j<2^w$，计算 $iP+jQ$;

(2) 令 $k=(K^{d-1},\cdots,K^1,K^0),l=(L^{d-1},\cdots,L^1,L^0),K^i,L^i$ 均是 w 长的比特串，$d=\lceil t/w\rceil$;

(3) R 为无穷远点；

(4) For i from $d-1$ downto 0 do

① $R\longleftarrow 2^wR$;

② $R\longleftarrow R+(K^iP+L^iQ)$;

(5) 返回 R.

利用滑动窗口，可以进一步提高该算法的效率. 在每个循环中，宽度至多为 w 的窗口由左向右移动，直至窗口的最右边非零，才进行操作. 其预存储减少为

$2^{2(w-1)}-1$ 个点，共需要约 $t/(w+(1/3))$ 次点加. 当 $w \in \{2,3\}$ 时，其运行时间约为算法 7.15 的 91%.

将 k,l 用 NAF 表示，以增加指数阵列中全零列的数量，则算法 7.15 所需的点加个数 (每次仅处理一列) 减少为 $5t/9$ 个. 适当选择 k,l 的有符号二进制表示，则全零列的个数会进一步增加. 整数对 k,l 的有符号二进制表示称为联合二进制表示，联合 Hamming 密度定义为非零列的个数与总列数的比值. 联合稀疏表示 JSF 是联合二进制表示中联合 Hamming 密度最小的，其期望值为 1/2. k,l 的 JSF 简记作 $\mathrm{JSF}(k,l)$，具有如下性质:

(1) 任意的连续三列中至少有一个全零列;

(2) 同行的相邻项符号不会不同;

(3) 若 $k_{j+1}k_j \neq 0$，则 $l_{j+1} \neq 0, l_j = 0$；若 $l_{j+1}l_j \neq 0$，则 $k_{j+1} \neq 0, k_j = 0$.

若在算法 7.15 中使用 JSF，且每次循环仅处理一列，则共需要 $t/2$ 次点加. 算法 7.16 描述了 k,l 的 JSF 求取过程.

算法 7.16 (JSF)

输入 不全为零的非负整数 k^1, k^2.

输出 $\mathrm{JSF}(k^1, k^2)$.

(1) $l \longleftarrow 0, d_1 \longleftarrow 0, d_2 \longleftarrow 0$;

(2) While ($k^1 + d_1 > 0$或$k^2 + d_2 > 0$) do

① $l_1 \longleftarrow d_1 + k^1, l_2 \longleftarrow d_2 + k^2$.

② For i from 1 to 2 do

若 l_i 为偶数，则 $u \longleftarrow 0$.

否则

$u \longleftarrow l_i \bmod\mathrm{s}\ 4$.

若 $l_i \equiv \pm 3 \mod 8$且$l_{3-i} \equiv 2 \mod 4$，则 $u \longleftarrow -u$.

$k_l^i \longleftarrow u$.

③ For i from 1 to 2 do

若 $2d_i = 1 + k_l^i$，则 $d_i \longleftarrow 1 - d_i$; $k^i \longleftarrow \lfloor k^i/2 \rfloor$;

④ $l \longleftarrow l + 1$;

(3) 返回 $\mathrm{JSF}(k^1, k^2) = \begin{pmatrix} k_{l-1}^1, & \cdots, & k_0^1 \\ k_{l-1}^2, & \cdots, & k_0^2 \end{pmatrix}$.

Avanzi[8] 结合了 JSF 和窗口技术，将平均联合 Hamming 密度减少为 3/8.

设 k 是 t 比特整数，令 $d=\lceil t/2\rceil, Q=2^dP$ ，则 $kP=k^1P+k^2Q, k^1, k^2$ 为 d 比特整数，即可以利用双标量乘法的快速算法来实现标量乘法，其与 $w=2$ 的固定梳形算法的效率比较请见表 7.3：

表 7.3 梳形算法的效率

算法	存储量	点加	倍点
固定梳形	3	$3t/8\approx .38t$	$t/2$
算法 7.16	4	$t/4\approx .25t$	$t/2$

7.3.2 JSF$_3$

本小节将给出一种新的联合稀疏表示. 设 k 的 3 窗口广义二进制表示为 $(k_{l-1},\cdots,k_1,k_0)_3$ ，显然若 k 是偶数，则 $k_0=0$；若 k 是奇数，则

$$k_0\in\{k\text{mods } 8,(k+4)\mod 8,-(k\text{mods } 8),-((k+4)\text{mods } 8)\},$$

当 $k_0=k\text{mods } 8$ 时称 k_0 取原值 (FOV(k))，当 $k_0=(k+4)\text{mods } 8$ 时称 k_0 取变反值 (FAV(k))，当 $k_0=-(k\text{mods } 8)$ 时称 k_0 取变号值 (FSV(k))，当 $k_0=-((k+4)\text{mods } 8)$ 时称 k_0 取变值值 (FNV(k)).

定义 7.3.1 整数 k_0,k_1 的 3 窗口联合广义二进制表示

$$k_0=(k_{0,m-1},\cdots,k_{0,1},k_{0,0}),$$
$$k_1=(k_{1,m-1},\cdots,k_{1,1},k_{1,0})$$

称为 3 窗口联合稀疏表示 (JSF$_3(k_0,k_1)$)，简记作 JSF$_3$，如果其具有下述性质：

(1) 任意连续三列至少一个为全零；任意连续五列至少两个为全零；

(2) 同行相邻项的乘积不是 -1；

(3) 若存在 $i\in\{0,1\}$ 满足 $k_{i,j}\neq 0, k_{i,j+1}\neq 0$，则 $k_{1-i,j+1}\neq 0, k_{1-i,j}=0$；

(4) 若存在 $i\in\{0,1\}$ 满足 $k_{i,j}\neq 0, k_{i,j+2}\neq 0$，则 $k_{1-i,j+2}\neq 0$.

JSF$_3$ 的平均联合 Hamming 密度约为 37.1%，将其和 Shamir 算法相结合，则 $kP+lQ$ 的实现效率比算法 7.16 提高了约 8.6%. 下面给出 JSF$_3$ 的求解算法，其有关细节可参见文献 [62].

算法 7.17 (JSF$_3$)

输入 不全为零的非负整数 k_0,k_1.

输出　$\mathrm{JSF}_3(k_0,k_1): k_i=(k_{i,m-1},\cdots,k_{i,1},k_{i,0}), k_{i,j}\in\{0,\pm1,\pm3\}, i=0,1, 0\leqslant j<m$.

(1) $j\longleftarrow 0$.

(2) While $k_0>0$或$k_1>0$ do

For i from 0 to 1 do

①若 k_i 是偶数，则 $u\longleftarrow 0$;

②否则 $u\longleftarrow \mathrm{FOV}(k_i)$;

若 k_{1-i} 为偶数，则

若 $k_{1-i} \mod 8=4$，则 $u\longleftarrow \mathrm{FAV}(k_i)$;

若 $k_{1-i} \mod 4=2$且$k_i \mod 32=\pm1,\pm3$，则 $u\longleftarrow \mathrm{FNV}(k_i)$;

若 $k_{1-i} \mod 4=2$且$k_i \mod 32=\pm5,\pm11$，则 $u\longleftarrow \mathrm{FSV}(k_i)$;

若 $k_{1-i} \mod 4=2$且$k_i \mod 32=\pm13,\pm15$，则 $u\longleftarrow \mathrm{FSV}(k_i)$;

若 $k_{1-i} \mod 32=\pm2,\pm6$且$k_i \mod 32=\pm7$，则 $u\longleftarrow \mathrm{FSV}(k_i)$;

若 $k_{1-i} \mod 32=\pm2,\pm6$且$k_i \mod 32=\pm9$，则 $u\longleftarrow \mathrm{FNV}(k_i)$;

若 $k_{1-i} \mod 32=\pm10,\pm14$且$k_i \mod 32=\pm7$，则 $u\longleftarrow \mathrm{FNV}(k_i)$;

若 $k_{1-i} \mod 32=\pm10,\pm14$且$k_i \mod 32=\pm9$，则 $u\longleftarrow \mathrm{FSV}(k_i)$;

否则

若 $k_i \mod 32=\pm13,\pm15$且$k_{1-i} \mod 16=\pm5,\pm7$，则 $u\longleftarrow \mathrm{FAV}(k_i)$;

若 $k_i \mod 16=\pm5,\pm7$且$k_{1-i} \mod 32=\pm13,\pm15$，则 $u\longleftarrow \mathrm{FAV}(k_i)$;

③ $k_{i,j}\longleftarrow u$.

$k_0\longleftarrow (k_0-k_{0,j})/2, k_1\longleftarrow (k_1-k_{1,j})/2$;

$j\longleftarrow j+1$;

(3) 输出 $(k_{i,j-1},\cdots,k_{i,1},k_{i,0}), i=0,1$.

7.4　Koblitz 曲线

Koblitz 曲线是特征为 2 基域上的一类特殊椭圆曲线，其优点之一是标量乘法的实现过程中不需要倍点运算．本节内容多取材于 Solinas 所著的文献 [132].

定义 7.4.1　Koblitz 曲线是定义在 $\mathbb{F}_2$ 上的如下曲线:

$$E_0: Y^2+XY=X^3+1;$$

$$E_1: Y^2+XY=X^3+X^2+1.$$

椭圆曲线密码体制有时将群 $E_0(\mathbb{F}_{2^m}), E_1(\mathbb{F}_{2^m})$ 作为其构建的基础. 设 $a \in \{0,1\}$. 对于 m 的任意因子 l，$E_a(\mathbb{F}_{2^l})$ 是 $E_a(\mathbb{F}_{2^m})$ 的子群, 所以 $|E_a(\mathbb{F}_{2^l})|$ 整除 $|E_a(\mathbb{F}_{2^m})|$. 而 $|E_0(\mathbb{F}_2)| = 4, |E_1(\mathbb{F}_2)| = 2$, 故 $|E_0(\mathbb{F}_{2^m})|$ 是 4 的倍数, $|E_1(\mathbb{F}_{2^m})|$ 是 2 的倍数.

定义 7.4.2 Koblitz 曲线在 $\mathbb{F}_{2^m}$ 上的阶为拟素数 (almost-prime) ，若$|E_a(\mathbb{F}_{2^m})| = hn$ ，其中 n 是素数，

$$h = \begin{cases} 4, & a = 0 \\ 2, & a = 1 \end{cases}$$

h 称为伴因子 (cofactor).

显然, 仅当 m 是素数时，$|E_a(\mathbb{F}_{2^m})|$ 才可能是拟素数. 本节均假设 E_a 是 Koblitz 曲线，$|E_a(\mathbb{F}_{2^m})|$ 是拟素数.

若 $\mathbb{F}_{2^m}$ 中的元素用正规基表示, 则 Frobenius 映射

$$\phi : E_a(\mathbb{F}_{2^m}) \to E_a(\mathbb{F}_{2^m}),$$
$$(x, y) \mapsto (x^2, y^2)$$

只需移位便可实现. 由 $\phi^2 - \mu\phi + 2 = 0, \mu = (-1)^{1-a}$ 可知存在复数 $\tau = (\mu + \sqrt{-7})/2$ 使得 $\phi(P) = \tau P$, 其中 $P \in E_a(\mathbb{F}_{2^m})$, 所以对于 $u_{l-1}\tau^l + \cdots + u_1\tau + u_0 \in \mathbb{Z}[\tau]$ 有

$$(u_{l-1}\tau^{l-1} + \cdots + u_1\tau + u_0)P = u_{l-1}\phi^{l-1}(P) + \cdots + u_1\phi(P) + u_0P.$$

任意正整数 k 均有 τ 表示为

$$k = \sum_{i=0}^{l-1} u_i\tau^i, \qquad u_i \in \{0, \pm 1\},$$

u_i 是将 k 不断地用 τ 相除所得的余数. 为减少点加个数, 可将非相邻二进制表示推广为非相邻 τ 表示:

定义 7.4.3 非零元素 $k \in \mathbb{Z}[\tau]$ 的非相邻 τ 表示为

$$k = \sum_{i=0}^{l-1} u_i\tau^i, \qquad u_i \in \{0, \pm 1\}, u_{l-1} \neq 0,$$

且相邻两项中至少一个为零. l 称为 NAF_τ 的长度.

对于非零元素 $k \in \mathbb{Z}[\tau]$ ，存在唯一的非相邻 τ 表示，记作 $\mathrm{NAF}_\tau(k)$ ，其长度约为 $\log_2 N(k) = 2\log_2 k, N(k)$ 为 k 与其共轭的乘积． l 长的非相邻 τ 表示的平均 Hamming 密度为 1/3. 在 $\mathrm{NAF}_\tau(k)$ 的求取过程中，用 τ 除以 k ，若有余数，则选择 $r \in \{-1, 1\}$ ，使得 $(k-r)/\tau$ 能被 τ 整除，以确保下一分位为 0.

算法 7.18 (NAF_τ)

输入　$k = r_0 + r_1\tau \in \mathbb{Z}[\tau]$.

输出　$\mathrm{NAF}_\tau(k)$.

(1) $i \longleftarrow 0$;

(2) While $r_0 \neq 0$或$r_1 \neq 0$ do

①若 r_0 是奇数，则 $u_i \longleftarrow 2 - (r_0 - 2r_1 \mod 4), r_0 \longleftarrow r_0 - u_i$;

②否则， $u_i \longleftarrow 0$;

③ $t \longleftarrow r_0, r_0 \longleftarrow r_1 + \mu r_0/2, r_1 \longleftarrow -t/2, i \longleftarrow i+1$;

(3) 返回 $(u_{i-1}, u_{i-2}, \cdots, u_1, u_0)$.

因为 $(\phi^m - 1)(P) = O$ ， O 为无穷远点，所以若 $\gamma \equiv k \mod (\tau^m - 1)$ ，则 $kP = \gamma P$. 对于 $E_a(\mathbb{F}_{2^m})$ 中所有的 n 阶点 P ，若 $\rho \equiv k \mod \delta, \delta = (\tau^m - 1)/(\tau - 1)$ ，则 $kP = \rho P$ ，基于该事实，为了进一步提高实现效率，寻找 $\rho \in \mathbb{Z}[\tau]$ ，使得 $\rho \equiv k \mod \delta$ 且 $N(\rho)$ 尽可能小，从而求取 kP 转化为求取 ρP ，而 $\mathrm{NAF}_\tau(\rho)$ 长度较短. 算法 7.19 描述了 ρ 的计算过程， Solinas 证明了 $\mathrm{NAF}_\tau(\rho)$ 的长度不大于 $m + a$. 对于复数 $\lambda_0 + \lambda_1\tau, \lambda_0, \lambda_1 \in \mathbb{Q}$ ，算法 7.20 可以求得 $\mathbb{Z}[\tau]$ 中与其相近的元素.

算法 7.19

输入　$\alpha = a_0 + a_1\tau \in \mathbb{Z}[\tau], \beta = b_0 + b_1\tau \in \mathbb{Z}[\tau], \beta \neq 0$.

输出　$\kappa = q_0 + q_1\tau, \rho = r_0 + r_1\tau \in \mathbb{Z}[\tau]$ 满足 $\alpha = \kappa\beta + \rho, N(\rho) \leqslant \frac{4}{7}N(\beta)$.

(1) $g_0 \longleftarrow a_0b_0 + \mu a_0b_1 + 2a_1b_1$;

(2) $g_1 \longleftarrow a_1b_0 - a_0b_1$;

(3) $N \longleftarrow b_0^2 + \mu b_0b_1 + 2b_1^2$;

(4) $\lambda_0 \longleftarrow g_0/N, \lambda_1 \longleftarrow g_1/N$;

(5) 调用算法 7.20 计算 $(q_0, q_1) \longleftarrow \mathrm{Round}(\lambda_0, \lambda_1)$;

(6) $r_0 \longleftarrow a_0 - b_1q_0 + 2b_1q_1$;

(7) $r_1 \longleftarrow a_1 - b_1q_0 - b_0q_1 - \mu b_1q_1$;

(8) $\kappa \longleftarrow q_0 + q_1\tau$;

(9) $\rho \longleftarrow r_0 + r_1\tau$;

(10) 返回 κ, ρ.

算法 7.20 (Round)

输入 有理数 λ_0, λ_1.

输出 整数 q_0, q_1 满足 $q_0 + q_1\tau$ 接近于 $\lambda_0 + \lambda_1\tau$.

(1) For i from 0 to 1 do

$f_i \longleftarrow \left\lfloor \lambda_i + \dfrac{1}{2} \right\rfloor, \eta_i \longleftarrow \lambda_i - f_i, h_i \longleftarrow 0$;

(2) $\eta \longleftarrow 2\eta_0 + \mu\eta_1$;

(3) 若 $\eta \geqslant 1$ 则:

①若 $\eta_0 - 3\mu\eta_1 < -1$ ，则 $h_1 \longleftarrow \mu$. 否则 $h_0 \longleftarrow 1$;

②若 $\eta_0 + 4\mu\eta_1 \geqslant 2$ ，则 $h_1 \longleftarrow \mu$;

(4) 若 $\eta < -1$ 则:

①若 $\eta_0 - 3\mu\eta_1 \geqslant 1$ ，则 $h_1 \longleftarrow -\mu$. 否则 $h_0 \longleftarrow -1$;

②若 $\eta_0 + 4\mu\eta_1 < -2$ ，则 $h_1 \longleftarrow -\mu$;

(5) $q_0 \longleftarrow f_0 + h_0, q_1 \longleftarrow f_1 + h_1$;

(6) 返回 q_0, q_1.

定义 7.4.4 设 $\alpha, \beta \in \mathbb{Z}[\tau], \beta \neq 0$ ，则算法 7.19 的输出 ρ 记作 $\alpha \mod \beta$.

算法 7.19 的第 4 步需要两次整数的多精度除法，这限制了该算法的使用. Solinas 给出了算法 7.21 ，其在不需要多精度除法的条件下可以求取 $\rho' \equiv k \mod \delta$ ，记作 $\rho' = k$ partmod δ. 他还证明了对于充分大的 C ， $\rho' = \rho$ 的概率大于 $1 - 2^{-(C-5)}$.

算法 7.21

输入 $k \in [1, n-1], C \geqslant 2, s_0 = d_0 + \mu d_1, s_1 = -d_1$ ，其中 $\delta = d_0 + d_1\tau$.

输出 $\rho' = k$ partmod δ.

(1) $k' \longleftarrow \lfloor k/2^{a-C+(m-9)/2} \rfloor$;

(2) $V_m \longleftarrow 2^m + 1 - |E_a(\mathbb{F}_{2^m})|$;

(3) For i from 0 to 1 do

① $g' \longleftarrow s_i \cdot k', j' \longleftarrow V_m \cdot \lfloor g'/2^m \rfloor$;

② $\lambda_i \longleftarrow \lfloor (g' + j')/2^{(m+5)/2} + \dfrac{1}{2} \rfloor / 2^C$;

(4) 调用算法 7.20 计算 $(q_0, q_1) \longleftarrow \text{Round}(\lambda_0, \lambda_1)$;

(5) $r_0 \longleftarrow k - (s_0 + \mu s_1)q_0 - 2s_1q_1, r_1 \longleftarrow s_1q_0 - s_0q_1$;

(6) 返回 $r_0 + r_1\tau$.

将非相邻 τ 表示和算法 7.21 应用于标量乘法中，便得到算法 7.22，其运行时间约为 $\frac{m}{3}A$.

算法 7.22 (标量乘法的 NAF_τ 算法)

输入 整数 $k \in [1, n-1], P \in E_a(\mathbb{F}_{2^m})$ 且阶为 n.

输出 kP.

(1) 调用算法 7.21 求取 $\rho' = k \text{ partmod } \delta$;

(2) 调用算法 7.18 求取 $\text{NAF}_\tau(\rho') = \sum\limits_{i=0}^{l-1} u_i\tau^i$;

(3) Q 为无穷远点;

(4) For i from $l-1$ downto 0 do

① $Q \longleftarrow \tau Q$;

②若 $u_i = 1$，则 $Q \longleftarrow Q + P$;

③若 $u_i = -1$，则 $Q \longleftarrow Q - P$;

(5) 返回 Q.

定义 7.4.5 设正整数 $w \geqslant 2$，$\alpha_i = i \mod \tau^w, i \in \{1, 3, 5, \cdots, 2^{w-1} - 1)$，非零元素 $\kappa \in \mathbb{Z}[\tau]$ 的 w 窗口 NAF_τ 表示为

$$\kappa = \sum_{i=0}^{l-1} u_i\tau^i, u_i \in \{0, \pm\alpha_1, \pm\alpha_3, \cdots, \pm\alpha_{2^{w-1}-1}\}, u_{l-1} \neq 0,$$

且任何的连续 w 项中至多一个非零. l 为 $\text{NAF}_{\tau,w}(\kappa)$ 的长度.

设 $\{U_k\}$ 是整数列，$U_0 = 0, U_1 = 1, U_{k+1} = \mu U_k - 2U_{k-1}$，令 $t_k = 2U_{k-1}U_k^{-1} \mod 2^k$，则 $t_k^2 + 2 \equiv \mu t_k \mod 2^k$. 算法 7.23 可以高效求取 $\text{NAF}_{\tau,w}(\rho)$. 算法 7.24 是利用了 w 窗口 NAF_τ 表示的标量乘法计算过程，由于 $\text{NAF}_\tau(\rho)$ 的长度约为 m，$\text{NAF}_{\tau,w}$ 的 Hamming 密度约为 $1/(w+1)$，所以该算法的运行时间约为

$$\left(2^{w-2} - 1 + \frac{m}{w+1}\right)A.$$

算法 7.23

输入 $w, t_w, \alpha_u = \beta_u + \gamma_u\tau, u \in \{1, 3, 5, \cdots, 2^{w-1}-1\}, \rho = r_0 + r_1\tau \in \mathbb{Z}[\tau]$.

输出 $\text{NAF}_{\tau,w}(\rho)$.

(1) $i \longleftarrow 0$.

(2) While $r_0 \neq 0$或$r_1 \neq 0$ do

①若 r_0 是奇数，则

$u \longleftarrow r_0 + r_1 t_w \mod 2^w$;

若 $u > 0$ 则 $s \longleftarrow 1$. 否则 $s \longleftarrow -1, u \longleftarrow -u$;

$r_0 \longleftarrow r_0 - s\beta_u, r_1 \longleftarrow r_1 - s\gamma_u, u_i \longleftarrow s\alpha_u$;

②否则 $u_i \longleftarrow 0$;

③ $t \longleftarrow r_0, r_0 \longleftarrow r_1 + \mu r_0/2, r_1 \longleftarrow -t/2, i \longleftarrow i+1$;

(3) 返回 $(u_{i-1}, u_{i-2}, \cdots, u_1, u_0)$.

算法 7.24 (标量乘法的窗口 NAF_τ 算法)

输入 $w, k \in [1, n-1], n$ 阶点 $P \in E_a(\mathbb{F}_{2^m})$.

输出 kP.

(1) 调用算法 7.21 求取 $\rho' = k \text{ partmod } \delta$.

(2) 调用算法 7.23 求取 $\mathrm{NAF}_{\tau,w}(\rho') = \sum_{i=0}^{l-1} u_i \tau^i$;

(3) 计算 $P_u = \alpha_u P, u \in \{1, 3, 5, \cdots, 2^{w-1} - 1\}$;

(4) Q 为无穷远点;

(5) For i from $l-1$ downto 0 do

① $Q \longleftarrow \tau Q$;

②若 $u_i \neq 0$，则:

设 u 满足 $\alpha_u = u_i$ 或 $\alpha_{-u} = -u_i$;

若 $u > 0$ 则 $Q \longleftarrow Q + P_u$;

否则 $Q \longleftarrow Q - P_{-u}$;

(6) 返回 Q.

参 考 文 献

1 Adleman L M, Huang M D. Algorithmic Number Theory. LNCS 877, Berlin. Springer-Verlag

2 ANSI. Agreement of symmetric keys on using Diffie-Hellman and MQV algorithms. Working draft American National Standard: Public key cryptography for the financial services industry X9.42-1998, American National Standards Institute. http://grouper.ieee.org /groups /-1363/private/x9-42-10-02-98.zip

3 ANSI. The elliptic curve digital signature algorithm(ECDSA). Working draft American National Standard: Public key cryptography for the financial services industry X9.62-1998, American National Standards Institute. http://grouper.ieee.org /groups/1363/private/x9-62-09-20-98.zip

4 ANSI. Key agreement and key transport using elliptic curve cryptography. Working draft American National Standard: Public key cryptography for the financial services industry X9.63-199x, American National Standards Institute. http://grouper.ieee.org/groups/1363/private/x9-63-01-08-99.zip

5 Atkin A C L. The Number of Points on an Elliptic Curve Modulo a Prime. Series of E-mails to the NMBRTHRY Mailing List, 1988

6 Atkin A O L. The Number of Points on an elliptic Curve Modulo a Prime(ii). Series of E-mails to the NMBRTHRY Mailing List, 1992

7 Atkin A O L, Morain F. Elliptic curves and primality proving. Mathematics of Computation,1993, 61(203):29～68

8 Avanzi R. On multi-exponentiation in cryptography. 2003, manuscript, http: //citeseer. nj. nec.com/545130.html

9 Blake I F,Fuji-Hara R,Mullin R C, Vanstone S A. Computing logarithms in finite fields of characteristic two. SIAM J. Alg. Disc. Math., 1984,5(2):276～285

10 Blake I, Sercussi G, Smart N. Elliptic Curve in Cryptography. Cambridge Univ. Press, 1999

11 Borel A et al. Seminar on Complex Multiplication. No. 21 in Lect. Notes in Math. Springer,1966

12 Brent R P. An improved Monte Carlo factorization algorithm. BIT, 1980,20: 176～184

13 Brickell E F. Advances in Cryptology-CRYPTO 1992. LNCS 740, Berlin. Springer-Verlag.1992

14 Buell D A, Teitelbaum J T. Computational perspectives on number theory: Proceeding of a Conference in Honor of Atkin A O L, Vol.7 of Studies in Advanced Mathematics. American Mathematical Society. 1998

15 Certicom. ECC challenge. http://www.certicom.com/chal/index.htm.1997

16 Charlap L S, Robbins D P. An elementary introduction to elliptic curves. CRD Expository Report 31, Institute for Defense Analyses, Princeton.1988

17 Charlap L S, Coley R. An elementary introduction to elliptic curve II, CCR Expository Report, 1990,8(34)

18 Cohen H. A Course in Computational Algebraic Number Theory.Springer-Verlag. 1999

19 Cohen H. Algorithmic Number Theory-ANTS-II. LNCS 1122, Berlin, Springer-Verlag. 1996

20 Coppersmith D. Fast evaluation of logarithms in fields of characteritic two. IEEE Transactions on Information Theory, 1984, 30(4): 587~594

21 Csirik J A. Counting the number of points on an elliptic curve on a low-memory device. The 2nd Elliptic Curve Cryptography Workshop (ECC 1998), http://www.csirik.net/papers.html

22 Cornacchia G. Su dī un metodo per la risoluzione in numeri interi dell' equazione $\sum_{h=0}^{n} C_h x^{n-h} y^h = P$. Giornale di Matematiche di Battaglini 1908(46),33~90

23 Couveignes J M. Computing l-isogenies with the p-torsion. ANTS-II Lecture Notes in Comp. Sci., 1996, 1122: 59

24 Couveignes J M. Quelques calculs en théorie des nombres. PhD thesis, Université de Bordeaux I. http://www.ufr-mi.u-bordeaux.fr/ couveign/Publi/Cou94-4.ps.1994

25 Couveignes J M, Dewaghe L, Morain F. Isogeny cycles and the Schoof-Elkies-Atkin algorithm. Technical Report LIX/RR/96/03,Laboratoire d'Informatique de l'Ecole Polytechnique(LIX), Palaiseau.ftp://lix.polytechnique.fr/pub/submissions/morain/Preprints/isogcycles. ps. Z. 1996

26 Couveignes J M, Morain F. Schoof's algorithm and isogeny cycles, 1994, 1: 43~58

27 Deuring M. Die Typen der Multiplikatorenringe elliptischer Funktionenkörper. Abhandlungen aus dem Mathematischen Seminar der Hamburgischen Universität, 1941,14:197~272

28 Diffie W, Hellman M E. New directions in cryptography. IEEE Transactions on Information Theory, 1976, 22(6): 644~655

29 ElGamal T. A public key cryptosystem and a signature scheme based on discrete logarithms. IEEE Transactions on Information Theory, 1985, 31(4): 469~472

30 Elkies N D. Elliptic and modular curves over finite fields and related computational issues. Computational Perspectives on Number Theory, 1998: 21~76

31 Enge A. Computing discrete logarithms in high-genus hyperelliptic Jacobians in provably subexponential time. Submitted to Mathematics of Computation. 1998

32 Enge A. Elliptic Curve and Their Applications to Cryptography: An Introduction. Kluwer Academic Publishers, 1999

33 Escott A. Implementing a parallel pollard rho attack on ECC. Transparencies of the Presentation Given at the 2nd Workshop on Elliptic Curve Cryptography at the University of Waterloo. htpp://cacr.math.uwaterloo.ca/escott.ps.zip.1998

34 Fouquet M et al. An extension of Satoh's algorithm and its implementation. J. Ramanujan Math. Soc., 2000, 15:281

35 Fouquet M et al. Finding secure curves with the Satoh-FGH algorithm and an early-abort strategy. Eurocrypto 2001, LNCS 2045, 14~29

36 Frey G, Rück H G. A remark concerning m-divisibility and the discrete logarithm in the divisor class group of curves. Mathematics of Computation, 1994, 62(206):865~874

37 Fulton W. Algebraic Curves. Mathematics Lecture Note Series. The Benjamin/Cummings Publishing Company, Reading(Massachusetts).1969

38 Fumy W. Advances in Cryptology-EUROCRYPT 1997, LNCS1233, Berlin. Springer-Verlag. 1997

39 Gallant R,Lambert R, Vanstone S. Improving the Parallelized Pollard Lambda Search on Binary Anomalous Curves. Preprint

40 Gaudry P. A comparision and a combination of SST and AGM algorithms for counting points of elliptic curves in characteristic 2. Asiacrypt'2002, LNCS 2501, 311~327

41 Gauß C F. Disquistiones Arithmeticae. Gerh. Fleischer Jun., Leipzig.1801

42 Gillings R J. Mathematics in the Time of the Pharaohs. MIT Press, Cambridge(Massachusette). 1972

43 Goldwasser S, Kilian J. Almost all primes can be quickly certified. Proc. 18th STOC, ACM, 1986, 316~329. Berkeley

44 Gordon D M. Discrete logarithms in GF(p) using the number field sieve. SIAM Journal on Discrete Mathematics,1993, 6(1):124~138

45 Gordon D M, McCurley K S. Massively parallel computation of discrete logarithms. In [13], 312~323

46 Hall M Jr. The Theory of Groups. Macmillan,New York. 1959

47 Hankerson B, Menezes A, Vanstone S. Guide to Elliptic Curve Cryptography. Springer-Verlag. New York. 2004

48 Harley R. Counting points with the arithmetic-geometric mean (joint work with J. F. Mestre and P. Gaudry). Eurocrypto' 2001, Rump session

49 Hasse H.Abstrakte Begrundung der komplexen Multiplikation und Riemannsche Vermutung in Funktionenkörpern. Abhandlungen aus dem mathematischen Seminar der hamburgischen Universitöt,1934, 10:325~348

50 Horster P, Michels M, Petersen H. Meta-ElGamal signature schemes based on the discrete logarithm problem, Technical Report TR-94-6, Theoretical Computer Science and Information Security, TU Chemnitz-Zwickau, June, 1994: 5

51 Husemöller D. Elliptic Curves. Graduate Texts in Mathematics. Springer-Verlag, New York.1987

52 IEEE. Standard specifications for public key cryptography. Technical Report P1363/D8.Institute of Electrical and Electronics Engineering. http://grouper.ieee.org/groups/1363/index.html.1998

53 Izu T et al. Efficient implementation of Schoof's algorithm. Asiacrypt' 1998, 66~79

54 Jacobson M J,Koblitz N,Silverman J H, Teske E. Analysis of the Xedni Calculus Attack. Preprint. 1999

55 Johnson D S, Nishizeki T, Nozaki A, Wolf H S. Discrete Algorithms and Complexity, Proceedings of the Japan-US Joint Seminar, June 4~6, 1986, Kyoto, Japan, Perspectives in Computing, Orlando. Academic Press. 1987, 15

56 Knuth D E. The art of computer programming. Seminumerical Algorithms. Addison-Wesley, Reading(Massachusetts), 2nd edition. 1981, 2

57 Koblitz N. Elliptic curve cryptosystems. Mathematics of computiation, 1987, 48(177): 203~209

58 Koblitz N. Constructing elliptic curve cryptosystems in characteristic 2. In [88], 1991: 156~167

59 Koblitz N. Introduction to Elliptic Curves and Modular Forms. Graduate Texts in Mathematics. Springer-Verlag, New York, 2nd edition. 1993

60 Koblitz N. A Course in Number Theory and Cryptography. Graduate Texts in Mathematics. Springer-Verlag, New York, 2nd edition. 1994

61 Koblitz N. Algebraic Aspects of Cryptography. Vol.3 of Algorithms and Computations in Mathematics. Springer-Verlag, Berlin. 1998

62 Kuang Bai-jie, Zhu Yue-fei, Zhang Ya-juan. An Improved Algorithm for uP+vQ Using JSF_3, LNCS 3089, ACNS 2004, Springer-Verlag, 467~478

63 Lang S.Elliptic curves: Diophantine Analysis. Vol.231 of Grundlehren der Mathematischen Wissenschaften. Springer-Verlag, Berlin. 1978

64 Lang S. Elliptic Functions.Graduate Texts in Mathematics. Springer-Verlag, New York, 2nd edition. 1987

65 Lay G J, Zimmer H G. Constructing elliptic curves with given group order over large finite fields. In [1], 1994, 250~263

66 Lehmann F, Maurer M, Muller V, Shoup V. Counting the number of points on elliptic curves over finite fields of characteristic greater than three. In [1], 1994, 60~70

67 Lehmann F J. Implementierung von Algorithmen zur Berechnung modularer Polynome und deren Anwendung im Algorithmus von Atkin. Master's thesis, Universität des Saarlandes, Saarbrucken. ftp://ftp.informatik.tu-darmstadt. de /pub /TI /reports /lehmann. diplom. ps. gz. 1994

68 Lenstra H W. Factoring integers with elliptic curves. Ann. Math., 1987, 126: 649~673

69 Lenstra H W Jr. Elliptic curves and number theoretic algorithms. Tech. Rep. Report 86~19, Math. Inst., Univ. Amsterdam, 1986

70 Lercier R. Computing isogenies in GF(2^n). In [19], 1996, 197~212

71 Lercier R. Algorithmique des courbes elliptiques dans les corps finis. PhD thesis,École polytechnique, Palaiseau. ftp://lix.polytechnique.fr/pub/lercier/papers/these.ps.Z.1997

72 Lercier R. Finding good random elliptic curves for cryptosystems defined over $\mathbb{F}_{2^n}$. In [38], 1997, 379~392

73 Lercier R et al. Counting the number of points on elliptic curves over finite fields: strategies and performances. Eurocrypto'1995, LNCS 2045, 79~94

74 Lercier R, Morain F. Algorithms for computing isogenies between elliptic curves. To Appear in Computational Perspectives on Number Theory, 1997. ftp: //lix. polytechnique.fr/pub/ submissions /morain /Preprints /isogenies. ps. Z and ftp: //lix. polytechnique. fr /pub/ lercier /papers /isogenies. ps. Z. 1996

75 Lewis D. Proceedings of symposia in pure mathematics. Vol.10, Providence(Rhode Island). American Mathematical Society.1971

76 Lovorn R Bender. Rigorous, subexponential algorithms for discrete logarithms in GF(p^2). To Appear in SIAM J. Discrete Math.1999

77 Lubin J, Serre J P, Tate J. Elliptic curves and formal groups. In Lecture notes prepared in connnection with the seminars held at the Summer Insitute on Algebraic Geometry, Whitney Estate, Woods Hole, Massachusetts, July 6-July 21, 1964. http://www.ma.utexas.edu/ users/voloch/1st.html

78 Marc Skov Madsen. The AGM-method of point counting on ordinary elliptic curves over finite fields of characteristic 2. Preprint, 2002

79 Martin R, McMillen W. An elliptic curve over $\mathbb{Q}$ with rank at least 23. Posting to the Number Theory List. http://listserv. nodak. edu /archives /nmbrthry. html. 1997

80 Maurer M. Eine Implementierung des Algorithmus von Atkin zur Berechnung der Punktanzahl elliptischer Kurven über endlichen Primkörpern der Charakteristik größer drei. Master's thesis, Universität des Saarlandes, Saarbrücken. ftp://ftp.informatik.tu-darmstadt.de /pub /TI/ reports /maurer. diplom. ps. gz. 1994

81 Maurer U M, Wolf S. On the complexity of breaking the Diffie-Hellman protocol. Technical Report 244, Institute for Theoretical Computer Science, ETH Zürich. ftp://ftp.inf.ethz.ch/pub/ publications/papers/ti/isc/Diffie_Hellman_DL_TR. ps. gz. 1996

82 McCurley K S. Cryptographic key distribution and computation in class groups. In [93], 459～479. 1989

83 Menezes A. Applications of Finite Fields. Kluwer Academic Publishers, Boston /Dordrecht/ London. 1993

84 Menezes A. Elliptic curve public key cryptosystems. Kluwer Academic Publishers. Boston/ Dordrecht /London. 1993

85 Menezes A, Vanstone S. Isomorphism classes of elliptic curves over finite fields of characteristic 2.Utilitas Mathematica, 1990, 38: 135～153

86 Menezes A J, Okamoto T, Vanstone S A. Reducing elliptic curve logarithms to logarithms in a finite field. IEEE Transactions on Information Theory, 1993, 39(5): 1639～1646

87 Menezes A J, Oorschot P, Vanstone S A. Handbook of Applied Cryptography. CRC Press, Boca Raton. 1997

88 Menezes A J, Vanstone S A. Advances in Cryptology-CRYPTO 1990, LNCS537, Berlin. Springer-Verlag. 1991

89 Menezes A J, Vanstone S A, Zuccherato R J. Counting points on elliptic curves over $\mathbb{F}_{2^m}$. Mathematics of Computation, 1993, 60(201): 407～420

90 Mestre J F. Construction d'une courbe elliptique de rang $\geqslant 12$. Comptes Rendus des Séances de l'Académie des Sciences de Paris, Série I, 1982, 295: 643～644

91 Mestre J F. Formules explicites et minorations de condusteurs de variétés algébriques. Compositio Mathematica, 1986, 58: 209～232

92 Miller V S. Use of elliptic curves in cryptography. In [144], 1986, 417～426

93 Mollin R A. Number Theory and Applications. Vol.265 of NATO ASI Series C: Mathematical and Physical Sciences, Dordrecht. Kluwer Academic Publishers. 1989

94 Morain F. Classes d'isomorphismes des courbes elliptiques supersingulières en caractéristique $\geqslant 3$. Utilitas Mathematica, 1997, 52: 241～253

95 Morain F. Primality proving using elliptic curves: an update. In JP Buhler, editor, Algorithmic Number Theory, LNCS 1423, pp. 111～127. Springer-Verlag, 1998. Third International Symposium, ANTS-III, Portland, Oregon, june 1998, Proceedings

96 Müller V. Die Berechnung der Punktanzahl von elliptischen Kurven über endlichen Primkörpern. Master's thesis, Universität des Saarlandes, Saarbrücken. ftp://ftp.informatik.tu-darmstadt.de/ pub/TI/reports/vmueller.diplom.ps.gz.1991

97 Müller V. Ein Algorithmus zur Bestimmung der Punktanzahl elliptischer Kurven über endlichen Körpern der Charakteristik größer drei. PhD thesis, Universität des Saarlandes, Saarbrücken. ftp://ftp.informatik.tu-darmstadt.de /pub /TI /reports /vmueller.. diss. ps. gz. 1995

98 Müller V, Stein A, Thiel C. Computing discrete logarithms in real quadratic congruence function fields of large genus. To appear in Mathematics of Computation; http://www. informatik. tu-darmstadt. de /TI /Mitarbeiter /vmuller /ffdl. ps. gz. 1997

99 NIST. Digital signature standard(DSS). Federal Information Processing Standard Publication 186, National Institute of Standards and Technology. http://csrc. nist. gov /fips /fips186. ps. 1994

100 NIST.Secure hash standard. Federal Information Processing Standard Publication 180-1, National Institute of Standards and Technology. http://csrc. nist. gov /fips /fip180-1. ps. 1995

101 NIST. Digital signature standard(DSS). Federal Information Processing Standard Publication 186-1, National Institute of standards and Technology. http: //csrc. nist. gov /fips /fips1861. pdf. 1998

102 Ohta K, Pei D. Advances in Cryptology-ASISCRYPT 1998. LNCS1514, Berlin. Springer-Verlag. 1998

103 Oorschot P, Wiener M J. Parallel collision search with cryptanalytic applications. Journal of Cryptology, 1999, 12(1): 1～28

104 Pohlig S C, Hellman M E. An improved algorithm for computing logarithms over GF(p) and its cryptographic significance. IEEE Transactions on Information Theory, 1978, 24(1):106～110

105 Pollard J M. Monte Carlo methods for index computation (mod$p$). Mathematics of Computation, 1978, 32(143): 918～924

106 Pomerance C. Fast,rigorous factorization and discrete logarithm algorithms. In [55], 1987, 119～143

107 Rosser J B, Schoenfeld L. Approximate formulas for some functions of prime numbers. Illinois Journal of Mathematics, 1962, 6: 64～94

108 Rück H G. A note on elliptic curves over finite fields. Mathematics of Computation, 1987, 49(179): 301～304

109 Satoh T. The canonical lift of an ordinary ellitpic curve over a finite field and its point counting. Journal of the Ramanujan Mathematical Society,December 2000, 15: 483

110 Satoh T. On p-adic point counting algorithms for elliptic curves over finite fields. Algorithmic number theory, 5th international symposium, ANTS-V, Sydney, Australia, LNCS 2369, 2002, 43～66

111 Satoh T, Araki K. Fermat quotients and the polynomial time discrete log algorithm for anomalous elliptic curves. Commentarii Mathematici Universitatis Sancti Pauli, 1987, 47(1): 81～92

112 Satoh T et al. Fast computation of canonical lifts of elliptic curves and its application to point counting. Finite Fields and Their Applications, 2003(9): 89～101

113 Schirokauer O. Discrete logarithms and local units. Philosophical Transactions Royal Society London A, 1993, 345: 409～423

114 Schnorr C P, Lenstra H W Jr. A Monte Carlo factoring algorithm with linear storage. Mathematics of Computation, 1984, 43(167): 289～311

115 Schonhage A, Strssen V. Schnelle multiplikation grosser Zahlen. Computing, 1971, 7: 281～292

116 Schoof R. Elliptic curves over finite fields and the computation of square roots mod p. Mathematics of Computation, 1985, 44(170): 483～494

117 Schoof R. Nonsingular plane cubic curves over finite fields. Journal of Combinatorial Theory, A 1987, 46: 183~211

118 Schoof R. Counting points on elliptic curves over finite fields. Journal de Théorie des Nombres de Bordeaux, 1995, 7: 219~254

119 Semaev I A. Evaluation of discrete logarithms in a group of p-torsion points of an elliptic curve in characteristic p. Mathematics of Computation, 1998, 67(221): 353~356

120 Serre J P. Cours d'arithmetique. Presses universitaires de France, 1970

121 Serre J P. Corps locaux. Hermann, 1968

122 Shafarevich J R. Basic Algebraic Geometry. Die Grundlehren der mathematischen Wissenschaften. Springer-Verlag, Berlin. 1974

123 Shanks D. Class number, a theory of factorization and genera. In [75], 1971, 415~440

124 Shikata J, Zheng Y, Suzuki J, Imai H. Realizing the Menezes-Okamoto-Vanstone(MOV) reduction efficiently for ordinary elliptic curves. IEICE Trans. Fundamentals, Vol. E83-A, 2000, 4: 756~763

125 Shoup V. Lower bounds for discrete logarithms and related problems. In [38], 1997, 256~266

126 Silverman J H. The Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. Springer-Verlag, New York. 1986,113

127 Silverman J H. Advanced Topics in the Arithmetic of Elliptic Curves. Graduate Texts in Mathematics. Springer-Verlag, New York. 1994

128 Silverman J H. The xedni calculus and the elliptic curve discrete logarithm problem. Preprint; http://www.math.brown.edu/ jhs/Preprints/XedniCalculus.ps.gz.1998

129 Silverman J H, Suzuki J. Elliptic curve discrete logarithms and the index calculus. In [102], 1998, 110~125

130 Skjernaa B. Satoh's algorithm in characteristic 2. Math Com 2003(72), 477~487

131 Smart N P. The discrete logarithm problem on elliptic curves of trace one. To appear in Journal of Cryptology. 1999

132 Solinas J. Efficient arithmetic on Koblitz curves. Designs, Codes and Cryptography, 2000, 19: 195~249

133 Solinas J. Low-Weight Binary Representations for Pairs of Integers. CACR Technical Reports, CORR2001-41 University of Waterloo, 2001. 7

134 Stinson D R. Cryptography-Theory and Practice. Discrete Mathematics and its Applications. CRC Press, Boca Raton. 1995

135 Tate J. Endomorphisms of abelian varieties over finite fields. Inventiones Mathematicae, 1966, 2: 134~144

136 Teske E. Better random walks for Pollard's rho method. Technical Report CORR98-52, Center for Applied Cryptographic Research, University of Waterloo. http: //cacr. math. uwaterloo. ca /techreports /1998 /corr98-52. ps. 1998

137 UNCITRAL. Draft uniform rules on electronic signatures. Technical Report A/CN.9/WG.IV/ WP. 79, United Nations Commission on International Trade Law. http: //www. un. or. at/ uncitral /english /sessions /wg_ec /wp-79. htm. 1998

138 UNCITRAL. Electronic signatures. Technical Report A/CN.9/WG.IV/WP.80, United Nations Commission on International Trade Law. http://www. un. or. at/uncitral/english/sessions/wg_ec /wp-80. htm. 1998

139 Vélu J. Isogénies entre courbes elliptiques. Comptes Rendus de l'Académie des Sciences de Paris, Série A, 1971, 273:238~241

140 Vercautern F et al. A memory efficient version of Satoh's algorithm. Eurocrypto' 2001, LNCS 2045, 1~13

141 Waterhouse W C. Abelian varieties over finite fields. Annales Scientifiques de l'École Normale Supérieure, 4^4 Série, 1969, 2:521~560

142 Weber D. Computing discrete logarithms with the general number field sieve. In [19], 1996, 391~403

143 Wiener M J, Zuccherato R J. Faster attacks on elliptic curve cryptosystems. In Proceedings of SAC, Workshop on Selected Areas in Cryptography, Lecture Notes in Computer Science. 1998

144 Williams H C. Advances in Cryptology-CRYPTO 1985, LNCS218, Berlin. Springer-Verlag. 1986